2016-1287

United States Court of Appeals for the Federal Circuit

ENOVA TECHNOLOGY CORPORATION,

Appellant,

v.

SEAGATE TECHNOLOGY (US) HOLDINGS, INC.,
SEAGATE TECHNOLOGY LLC,

Appellees.

Appeal from the United States Patent & Trademark Office, Patent Trial and Appeal Board in Case No. IPR2014-00683.

OPENING BRIEF OF APPELLANT ENOVA TECHNOLOGY CORP.

DARRYL M. WOO
Principal Attorney
VINSON & ELKINS LLP
555 Mission Street, Suite 2000
San Francisco, CA 94105-2763
Telephone: 415.979.6900
Facsimile: 415.520.5377
dwoo@velaw.com

Counsel for Appellant

APRIL 18, 2016

CERTIFICATE OF INTEREST

Counsel for the Appellant, Enova Technology Corporation, certifies the following:

1. The full name of every party or amicus represented by me is:

    Enova Technology Corporation

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is:

    Not applicable.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

    Not applicable.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

    FENWICK & WEST LLP.: Hector J. Ribera, Robert A. Hulse, Phillip Haack

    VINSON & ELKINS LLP: Darryl M. Woo, Ajeet P. Pai, Jeffrey Han, Janice Le Ta, Nickou Oskoui

Dated: April 18, 2016

/s/ *Darryl M. Woo*
DARRYL M. WOO
VINSON & ELKINS LLP

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5(a), Appellant Enova Technology Corporation ("Enova") provides as follows: (a) No other appeal from the same proceeding was previously before this or any other appellate court; (b) The patent-at-issue, U.S. Patent No. 7,136,995 ("'995 Patent"), is the subject of a related proceeding between the parties, currently stayed, in the U.S. District Court for the District of Delaware, No. 1:13-cv-1011-LPS (filed June 5, 2013). The '995 Patent was previously the subject of litigation in *Enova Technology Corp. v. Initio Corp.*, No. 10-04-LPS (D. Del.) ("*Initio*"). That action settled before this appeal. *Id*. U.S. Patent No. 7,900,057, which is a continuation-in-part of U.S. Patent Application Ser. No. 09/704,769, which issued as the '995 Patent, is the subject of several appeals pending before this Court: Nos. 16-1749, 16-1751, and the unassigned appeal of *Seagate Technology (US) Holdings v. Enova Technology Corp.*, IPR2014-1297, Paper No. 51 (PTAB Feb. 4, 2016).

JURISDICTIONAL STATEMENT

This is an appeal of a Final Written Decision issued by the Patent Trial and Appeals Board ("Board") on September 2, 2015. (Appx1-60). Pursuant to 35 U.S.C. § 142 and Federal Circuit Rule 15(a)(1), Enova timely filed a notice of appeal on October 29, 2015. (Appx555-58). Exclusive jurisdiction is vested in this Court under 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. § 141.

ISSUES PRESENTED

(1) In the underlying *inter partes review* ("IPR"), did the Patent Trial and Appeal Board ("Board") err in finding all claims of the '995 Patent obvious where the requisite "data stream interceptor" claim element was not in the prior art and suggested only by the '995 Patent?

(2) In invalidating all claims of the '995 Patent, did the Board err in basing its decision on a new argument raised for the first time in Appellees Seagate Technology (US) Holdings, Inc. and Seagate Technology LLC's ("Seagate") Reply Brief, in contravention of 35 U.S.C. § 312(a)(3)?

(3) Did the Board err in instituting the IPR based on a preliminary finding of obviousness bereft of any consideration of objective evidence of non-obviousness, and then making a final written decision based on an analysis that was similarly superficial?

(4) Did the Board misapply the broadest reasonable interpretation standard of claim construction in adopting (a) an overbroad construction that read out other claim limitations; and (b) a construction based on a dictionary definition at odds with the intrinsic record?

STATEMENT OF THE CASE

Around 2004, Seagate approached Enova to incorporate Enova's patented encryption technology into its computer hard drives. (Appx339-40, Appx2555-57). For years, Enova provided technological know-how and assistance in licensing its patented products to Seagate (Appx2555-61, Appx339-40), and Seagate enjoyed considerable commercial success from this partnership. (Appx242-43, Appx339-43, Appx2336-55). Around 2008, however, Seagate abruptly ceased purchasing Enova's patented encryption products and opted instead to copy them. (Appx342-43).

Faced with suit (Appx135), Seagate petitioned for an IPR, *Seagate Technology (US) Holdings Inc. v. Enova Technology Corp.*, IPR2014-00683, Paper No.1 (PTAB Apr. 23, 2014), asserting that the Enova technology it previously used to differentiate its products from its competitors (Appx339-40, Appx2328), was instead no more than the obvious combination of two prior art references: *Nolan* (an encryption device for antiquated tape drive technology), and the SCSI-2 standard (a standard for a cable interface to connect storage devices). (Appx143, Appx573-88, Appx590-1057).

Enova appeals the Board's finding of obviousness based on this combination—one that not only lacked the patented functionality, but also would not have been pursued absent the improper, hindsight use of the '995 Patent as a

roadmap for picking and choosing prior art components. (Appx2486).

Moreover, when Enova's response to Seagate's IPR petition pointed out that Seagate's obviousness argument was technically flawed, (Appx312-20, Appx2456-64), Seagate—whose own expert admitted he had erred, (Appx301-302, Appx330-31, Appx2377-78)—did an about-face and articulated a completely new ground for invalidity in the Reply Brief to its IPR petition, (Appx359-360). The Board, in violation of its own procedural rules, then adopted this new argument in its final decision, failing in the process to give Enova a meaningful opportunity to be heard. (Appx26-29, Appx519:1-524:15).

The Board's erroneous invalidity analysis was compounded by its failure to consider Enova's significant objective evidence of non-obviousness (also known as "secondary considerations"), including evidence of industry praise, commercial success, licensing, and copying by Seagate and others. (Appx241-44, Appx336-45, Appx2493-2503). Rather, the Board instituted the IPR based on an obviousness determination bereft of any consideration of these indicia (Appx269-70). Having made up its mind at this institution stage, the Board then proceeded to base its final decision on a similarly flawed analysis, superficially dismissing all objective evidence, while crediting Seagate's attorney argument. (Appx42-55). In so doing, the Board twice ignored this Court's admonishment that such indicia must always be considered as a necessary safeguard against hindsight bias.

Indeed, the potential for hindsight bias could not be more dangerous than in the IPR context, in which the "broadest reasonable interpretation" claim construction standard ("BRI") is often misapplied, as here, by (a) adopting an overly broad construction of the term "input" that read out other limitations and was inconsistent with the intrinsic record and the district court's prior construction of the term (Appx14-15, Appx258); and (b) adopting a construction of the term "transparently" based on an extrinsic dictionary definition at odds with the intrinsic record (Appx13-14, Appx256-57, Appx2788).

The sum of these iniquities led to the invalidation of all 15 claims of the '995 Patent, a result that deprived Enova of the patent forming the very basis for the company's existence. (Appx58). So valuable is Enova's invention that it has been copied by Seagate and several other companies, one of which entered into a consent judgment of infringement. (Appx2719-21).

Applying the correct obviousness analysis and claim constructions, the Court should reverse, or in the alternative, vacate and remand with appropriate instructions.

STATEMENT OF FACTS

A. PARTIES

In 2000, Mr. Shuning Wann founded Enova, a pioneer in the development of real-time encryption technologies for securing data on a computer hard drive. (Appx2328). Encryption is a security technology for preserving the privacy and confidentiality of sensitive information, such as litigation documents, design documents, and medical records. (Appx567 col.1:13-15, 21-25). Such sensitive information is often stored unencrypted because prior-art encryption technologies were slow and not easy to use. (Appx567 col.1:15-18, col.1:42-55, col.1:66-2:3).

Mr. Wann applied for the ’995 Patent on November 3, 2000, and it issued on November 14, 2006. (Appx562). The ’995 Patent is directed to hardware “adapted to perform data encryption/decryption without compromising the overall system performance.” (Appx567 col.1:5-8).

Seagate manufactures hard drives, devices that store data for use on a computer. (Appx2551). Around 2005, Seagate approached Enova to incorporate Enova’s encryption technology into such products. (Appx2556). For years hence, Enova supplied its patented encryption products to Seagate along with its know-how. (Appx2556-57). Seagate sold its products with Enova’s technology at a premium over its otherwise identical non-encrypted disk drives, and touted Enova’s “full disk” encryption technology as a feature. (Appx2557-58). Around

2008, however, Seagate abruptly ceased its purchasing and opted instead to sell its drives with an infringing encryption solution. (Appx2560).

B. STATE OF THE PRIOR ART

At the time of the invention of the ’995 Patent, there were relatively few cryptographic applications to protect data. (Appx567 col.1:35-38). Those that did exist were software based and designed to perform cryptography at the file-level; that is, on individual files. (Appx567 col.1:35-40, Appx289-90). On the surface, encrypting only selected files instead of entire hard drives seems to make sense since not all data is confidential. (Appx567 col.1:40-42).

However, software-based, file-level cryptography has distinct disadvantages, such as being inherently slow because it consumes computer resources. (Appx289-90, Appx567 col.1:35-50, Appx2435-36). Worse still, file-level cryptography often requires manual intervention by users who may become confused and frustrated by the interactive steps required to encrypt a file. (Appx290, Appx567 col.1:47-51, Appx2436). Because file-level cryptography can compromise overall system performance and requires user intervention, users often faced a choice between having quick and easy access to data or the protection of encryption. (Appx290, Appx567 col.1:42-45, Appx2435-36).

Security for file-level cryptography is also easily compromised. Since file-level cryptography programs are controlled by a computer’s operating system, an

unauthorized user who can subvert access to the operating system can also subvert file-level cryptography. (Appx290, Appx567 col.1:55-62, Appx2436). Moreover, file-level cryptography can fail to encrypt automatically-created temporary files that might be stored openly in clear text on a hard drive. (Appx290, Appx567 col.1:45-47, Appx2436). Because of poor performance and simple forgetfulness, users often neglect to encrypt sensitive data, risking potential security breaches. (Appx290, Appx567 col.1:40-62, Appx2436).

C. ’995 PATENT & ENOVA’S X-WALL PRODUCTS

To address the need for greater security and ease-of-use, the ’995 Patent was invented to automatically encrypt data on-the-fly at the *hardware* level—encrypting all user data as it is written to or read from the “disk” or storage device where the data are stored—rather than at the file-level. (Appx568 col.3:37-38, Appx2436). This “full-disk” encryption system was designed to operate without compromising overall system performance and without user intervention. (Appx290, Appx567 col.1:35-2:3, Appx2436).

Illustrative claim 9 recites:

> A cryptographic device comprising:
>
> at least one data stream interceptor that distinguishes between command/control and data signal transfers;
>
> a main controller receiving ***input*** from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through ***based on the received input*** from said at least one data stream interceptor;

> ...
>
> at least one cipher engine adapted to ***transparently encrypt or decrypt*** at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

(Appx569 col.6:45-64) (emphases added). Figure 4, below, is a block diagram of the ’995 patented invention.

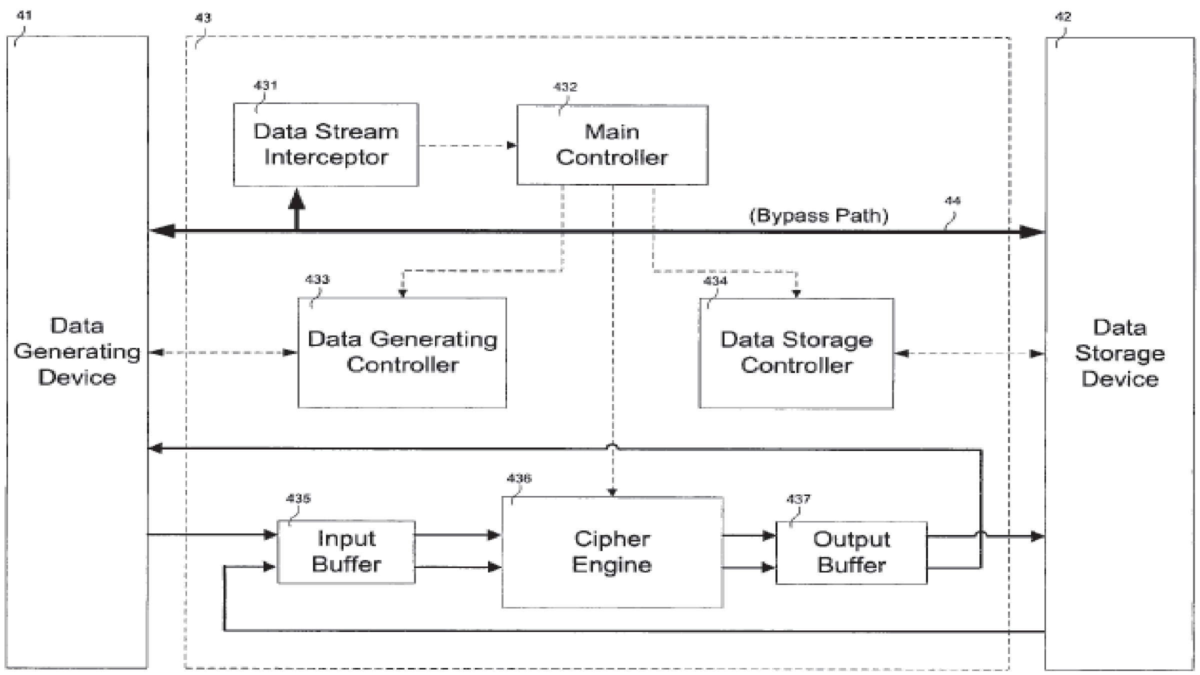


FIG. 4

(Appx566).

The patented cryptographic device is coupled between a “data generating device” (e.g., host computer) and a “data storage device” (e.g., hard drive). (Appx566, Appx568 col.3:10-12). The device automatically encrypts on-the-fly, as data is streaming (i.e., transmitted, loaded or saved) between the host computer

and disk drive. (Appx290, Appx2436).

To avoid encrypting a command or control signal in the data stream such that it cannot be understood by the storage device, the ’995 Patent claims a “data stream interceptor” that reads the incoming data streaming to/from the host computer and disk drive, distinguishes between command/control and data signal transfers, and provides this identification in the form of an input to the main controller. (Appx568 col.4:50-60, Appx2437). “Based on the received input,” the main controller then effectuates whether the incoming data, which may include commands/controls and data, should be encrypted, decrypted, or allowed to pass through without encryption. (Appx568 col.4:55-65, Appx2437).

Cipher engine 436 operates “transparently,” meaning that, “***[f]rom the functional viewpoint of data generating device [41] and/or data storage device [42]***, data transfers are being ***performed directly*** between data generating device [41] and/or data storage device [42], respectively, ***without any intervention by cryptographic device [43]***.” (Appx568 col.3:30-34).

This “transparent” design is at the heart of the ’995 Patent. Practically speaking, it means the invention does not tax the resources of the computer or hard drive, and encrypts automatically without any “apparent intervention by [the] cryptographic device.” (Appx568 col.3:24-37, col.4:1-2, col.4:25-29). The cryptographic device thus acts as an “‘invisible’ data transfer bridge” connecting

the data generating device and data storage device. (Appx568 col.3:34-37). This means the cryptographic device encrypts without requiring any resources or action from the host computer or the hard drive, neither of which are aware of this "invisible bridge." *Id.*

Furthermore, unlike file-level encryption software, Enova's invention teaches away from "requir[ing] manual intervention by users," such that data encryption is easy-to-use and automatic. (Appx567 col.1:47-55, 1:66-2:3).

In 2002, Enova introduced the commercial embodiments of the '995 Patent, its "X-Wall" line of Application *Specific* Integrated Circuit ("ASIC") products. The X-Wall Products were purpose-built to work securely and seamlessly (i.e., transparently) with computer hard drives to perform on-the-fly hardware encryption and had no other purpose than to practice the '995 patented invention. (Appx2328, Appx2493-94). These products were accordingly marked with the '995 Patent number and one or two additional but related patent numbers. (Appx2494-95, Appx2540-42, Appx2713).

D. SEAGATE ENJOYED CONSIDERABLE COMMERCIAL SUCCESS FROM LICENSING AND LATER COPYING ENOVA'S PRODUCTS

In 2005, Enova entered into an agreement by which Seagate purchased X-Wall ASICs, and the companies worked together to adapt them into Seagate's hard drives, including its Momentus product series. (Appx2555-56). The agreement contemplated quantities in the hundreds of thousands or millions of X-Wall ASICs,

and under it, Seagate acknowledged Enova as "the exclusive owner of certain Intellectual Property relating to the product known as the X-Wall® Chip." (Appx2557).

Seagate used Enova's technology to differentiate its products from its competitors, touting Enova's full disk encryption as providing "clear performance and reliability advantages," being "transparent to the user," and with lower costs. (Appx2337, Appx2339, Appx2570-71, Appx2499-2500). As a result, Seagate enjoyed considerable commercial success, selling over a million X-Wall encryption-enabled Momentus drives. (Appx242-243, Appx341-42, Appx2354-55, Appx2493, Appx2499-2501, Appx2540-42). Having received highly sensitive details about Enova's encryption technology, Seagate abruptly ceased purchasing X-Wall ASICs around 2007-2008 and opted instead to copy them. (Appx342, Appx2560).

E. *ENOVA V. INITIO*

Other competitors also copied the '995 patented invention. For example, after collaborating with Enova to incorporate X-Wall ASICs into its chip products, Initio Corporation began selling infringing products to major hard drive manufacturers including Western Digital and Buffalo. (Appx343-45, Appx2325, Appx2501-02). The resulting suit, *Enova v. Initio*, proceeded through claim construction. (Appx2321-23). The suit ended with Initio's entry into a consent

judgment of infringement, and Initio's hard drive manufacturers entering into settlements and licenses. (Appx54-55, Appx242, Appx344, Appx2324-25, Appx2501, Appx2679, Appx2686, Appx2690, Appx2696).

F. PROCEDURAL HISTORY

In 2013, Enova sued Seagate in the District of Delaware, alleging infringement of the '995 Patent by Seagate's full disk encryption Momentus and BlackArmor hard drives. (Appx2326). In response, Seagate petitioned for IPR. (Appx135).

IPRs were first introduced under the 2011 America Invents Act as an alternative means for challenging patents. America Invents Act, Pub. L. No.112-29, 125 Stat. 284 (2011). To seek *inter partes* review, patent challengers first petition the PTO. 35 U.S.C. §§ 311-312; 37 C.F.R. §§ 42.100-106. Under 35 U.S.C. § 312(a)(3), the petition must identify all grounds upon which the challenge is based. Seagate filed its petition on April 23, 2014, and a Corrected Petition ("Petition") on April 30, 2014. (Appx64-129, Appx130-94). Enova then filed its Preliminary Response to the Petition ("Preliminary Response"), on July 23, 2014. (Appx195-246; 35 U.S.C. § 313; 37 C.F.R. § 42.107).

During this institution stage, a three-judge panel of the Board decides whether there is a "reasonable likelihood" at least one claim will be invalidated. 35 U.S.C. § 314(a); 37 C.F.R. § 42.108. If so, the Board "institutes" the IPR. *Id*.

This institution decision is based on a limited record without the benefit of discovery, and the decision itself is non-reviewable. *See* 35 U.S.C. § 314(d); *In re Cuozzo Speed Techs., LLC,* 793 F.3d 1268, 1272-75 (Fed. Cir. 2015) (cert. granted). Here, the Board issued its Institution Decision on October 2, 2014 ("Institution Decision"). (Appx247-76; 35 U.S.C. § 314(a); 37 C.F.R. § 42.108).

After institution, Enova filed a further Response ("Response") (Appx277-352), and Seagate filed its Reply ("Reply") (Appx353-72). A patent owner is typically not permitted to file a written response to a petitioner's reply, and none was filed here. 37 C.F.R. 42.1-123 (containing no provisions for sur-reply).

An Oral Hearing is then conducted—often by, as in this instance, the same three-judge panel of the Board—and then a final written decision issues. 37 C.F.R. § 42.70. The scope of the hearing is constrained by the substantive arguments raised in the written submissions. *See* Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48768 (Aug. 14, 2012) ("A party … may only present arguments relied upon in the papers previously submitted."). Here, the Board conducted an oral hearing on May 11, 2015, ("Oral Hearing") and issued a Final Written Decision on September 2, 2015, declaring, as it did on institution, all claims of the '995 Patent unpatentable as obvious. (Appx1-60, Appx473-554).

SUMMARY OF ARGUMENT

The Court should reverse, or in the alternative, vacate and remand the

Board's determination of obviousness because (1) the Board erred in using the '995 Patent as a roadmap to piece together the "distinguishing" and "input-" providing functions of the "data stream interceptor," which are not disclosed by either of the *Nolan* or SCSI-2 references; (2) the Board erred in basing its obviousness determination on a new argument raised for the first time in Seagate's Reply; (3) the Board erroneously accorded no weight to the substantial objective evidence of non-obviousness by imposing an impossibly high, and legally incorrect, standard for "nexus," while giving undue weight to attorney argument and conjecture by Seagate; and (4) the Board misapplied the BRI standard in its constructions of "input" and "transparently," by, respectively, adopting an overbroad construction that reads out other claim terms or renders them surplussage, and adopting a dictionary definition at odds with the intrinsic record. Under the correct constructions, there is no evidence that *Nolan* reads on the patented invention.

ARGUMENT

A. STANDARD OF REVIEW

Seagate, the petitioner in the IPR, has the burden of proving unpatentability by a preponderance of evidence. 35 U.S.C. § 316(e). Obviousness is a question of law reviewed *de novo* with underlying factual findings reviewed for substantial evidence. *Crocs, Inc. v. ITC*, 598 F.3d 1294, 1308 (Fed. Cir. 2010). With regard

to claim construction, the Court reviews underlying factual determinations concerning extrinsic evidence for substantial evidence and the ultimate claim constructions *de novo*. *Teva Pharms. U.S.A., Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015). "An agency's interpretation of its regulations is neither entitled to deference nor given controlling weight if it is plainly erroneous or inconsistent with the regulation itself." *AMS Assocs. v. U.S.*, 737 F.3d 1338, 1343 (Fed. Cir. 2013).

B. THE COURT SHOULD REVERSE THE BOARD'S OBVIOUSNESS DETERMINATION, WHICH WAS BASED ON A PRIOR ART COMBINATION THAT LACKED THE PATENTED FUNCTIONALITY AND WOULD NOT HAVE BEEN PURSUED ABSENT THE IMPROPER USE OF THE '995 PATENT ITSELF AS A ROADMAP FOR PICKING AND CHOOSING PRIOR ART COMPONENTS

1. The Prior Art

a. Nolan

The Board held that claims 1-13 of the '995 Patent were unpatentable based on a combination of GB Patent App. No. 2,264,373A (Aug. 25, 1993) ("*Nolan*"), (Appx573-588), and the American National Standards Institute, SMALL COMPUTER SYSTEM INTERFACE-2 (1994) ("SCSI-2 standard"), (Appx590-1057). (*See* Appx16, Appx36, Appx40). In addition, the Board found claims 14 and 15 unpatentable based on these references in combination with two additional references. (Appx2).

Nolan discloses an encryption device designed for use with tape drives that use a Small Computer System Interface (SCSI). (Appx17-18, Appx579:13-15).

Figure 1, reproduced below, is a block diagram of the *Nolan* device. (Appx574).

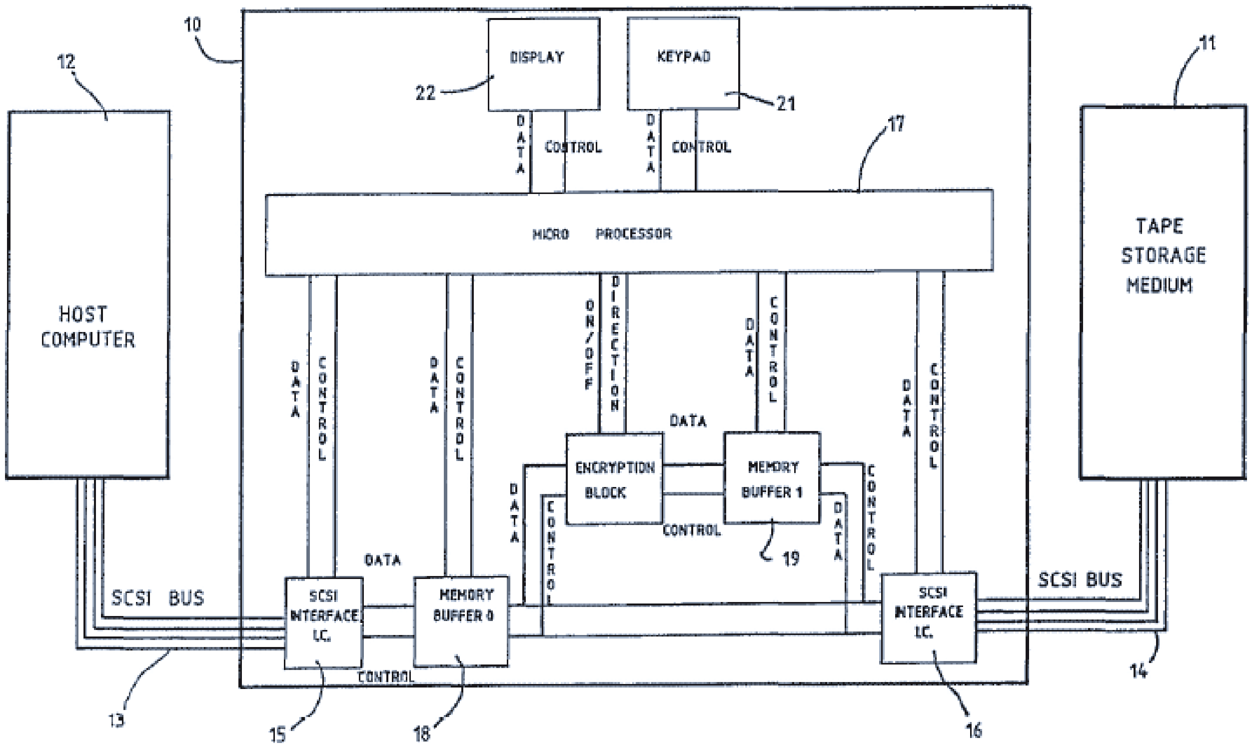


FIG 1

Nolan describes an "apparatus 10 for encrypting data to be stored on a tape 11…[that] includes [an encryption block] to encrypt different blocks of data using respective different keys which are derived from a common key." (Appx573). The encryption apparatus 10 is connected to a host computer 12 and tape drive storage medium 11 via a SCSI data bus 13 and 14. (Appx579:13-21). *Nolan* has a SCSI Interface 15 that can transfer data between the host computer 12 and the host memory buffer 18. (Appx579:25-580:1).

The encryption block in *Nolan* operates to encrypt data. (Appx580:23-581:1). To encrypt data, *Nolan* generates multiple encryption keys—complex

numbers that provide the formula for encryption. (Appx576, 578:1-6, 582:10-26). Generating the keys requires a user to first enter information into keypad 21 of the *Nolan* device. (Appx581:5-7). The *Nolan* device then writes and stores this key on the tape drive. (Appx581:5-9). Prior to encryption, the *Nolan* device must first request that the drive read the encryption key from the tape. (Appx581:14-18).

b. SCSI-2 Standard

SCSI-2 is a voluminous standard for a "data bus," a physical connection (cable) for transporting data and commands between computers and peripheral devices such as hard drives. (Appx18-20, Appx647, Appx623, Appx590-1057, Appx1841-42). The SCSI data bus is made of cables with over 50 conductors. (Appx1845). The SCSI-2 standard defines the mechanical, electrical, and functional characteristics of the cable connection. (Appx623).

SCSI-2 includes eight distinct phases that indicate the state of the SCSI data bus, i.e. what is being carried by the cable. (Appx19, Appx656). Of relevance to this appeal, four of these phases—the COMMAND, DATA, STATUS, and MESSAGE phases—are collectively referred as "information transfer phases" because "they are all used to transfer data or control information via the DATA BUS." (Appx19, Appx659-60).

2. The Combination of *Nolan* and the SCSI-2 Standard Does Not Teach or Suggest the Data Stream Interceptor for "Distinguishing Between Command/Control and Data Signal Transfers"

The Board construed the term "data stream interceptor" to mean "one or more components adapted to intercept at least one data stream and distinguish the command or control signals ***in the data stream*** from the data signals." (Appx11, Appx253-54).

Seagate contended that a data stream interceptor could be put together by combining *Nolan*'s disclosure of a SCSI Interface 15 with certain details of the SCSI-2 standard. (Appx20-21, Appx151). However, *Nolan* does not disclose how it "distinguish[es]" the command or control signals from the data signals; and the SCSI-2 standard says nothing about encryption. (Appx306-307).

Seagate had two theories as to how *Nolan* performed the claimed "distinguish[ing]" function. First, Seagate argued that *Nolan's* SCSI Interface 15, when implemented according to the SCSI-2 standard, satisfies the data stream interceptor limitation because it purportedly "intercepts" data travelling over the SCSI data bus and "distinguishes between command/control signals and data signals on the data bus based on the voltage level it sends and receives on a separate wire—called the 'Control/Data' wire." (Appx19, Appx154, Appx1132). Seagate argued this Control/Data wire ("C/D wire") accomplishes the "distinguishing" function by "indicat[ing] whether CONTROL or DATA

information is on the DATA BUS." (Appx649, Appx1115, Appx1117-18). According to Seagate, a higher voltage on the C/D wire indicates that command/control signals are being sent on the data bus, while a lower voltage indicates that data signals are being transmitted. (Appx154, Appx649, Appx1115, Appx1117-18).

Enova, in its Response, showed that the basis for this "C/D wire theory" was incorrect as contrary to the SCSI-2 documentation. (Appx301-02, Appx312-20, Appx2377:19-78:23). Importantly, Seagate's "C/D wire theory" assumed that ***only*** data signals can flow over the data bus in the (lower voltage) data phase, and ***only*** command/control signals can flow through the SCSI data bus in the (higher voltage) command/control phase, allowing the C/D wire to indicate one or the other of data signals or command/control signals by having, respectively, "lower" or "higher" voltages run through it. (Appx154, Appx301-02, Appx312-20, Appx1117-18).

Enova, however, pointed out that during the so-called "DATA phase," "other data, including command signals and control signals" may also flow through the SCSI-2 data bus. (Appx301-02, Appx312-19, Appx519-22). In other words, ***both*** command/control ***and*** data signals can flow through the SCSI data bus when the C/D wire is set to the so-called "DATA phase." *Id*. Thus, merely knowing that the SCSI interface is in a "DATA phase" is insufficient to distinguish

the command/control signals from the data signals because both data and command/control signals could be sent in that phase. *Id*. Indeed, during his deposition, Seagate's expert, Dr. Long, conceded that Seagate's C/D wire theory, along with Seagate's interpretation of the SCSI-2 standard, was incorrect. (Appx313, Appx520:3-32, Appx2377-78 ("Q: Your statement…is that during the data phase, only user data are sent over the data bus. [But] that's not correct, because there is additional data, not only user data? A: Right. There's additional data that could flow over the data bus and during the data phase. Q:…There can be data that flows during the data phase that should not be encrypted, correct? A: That's correct.").

After Enova's Response Brief pointed out this technical flaw in Seagate's "C/D wire" theory, (Appx289, Appx301-02), Seagate did an about-face and changed its theory of invalidity from a combination of *Nolan* and the C/D wire alone to one in which the "C/D [wire] is set ***in conjunction with*** [the] performance of the SCSI-2 operations READ(6) or WRITE(6)." (Appx359). By doing so, in its reply brief no less,[1] Seagate conceded that the C/D wire alone could not distinguish between command/control and data signals unless the devices happened to be carrying out certain READ and WRITE operations that purportedly open the data

[1] *See* Section B.5 below.

bus for the transfer of data signals (the "READ(6)/WRITE(6) theory"). (Appx359).

Significantly, only attorney argument[2] supported Seagate's new theory, as nothing in the declaration of Dr. Long explained Seagate's belated READ(6)/WRITE(6) theory. (Appx359). Rather, two conclusory sentences of Dr. Long's ninety-five page declaration vaguely mention non-descript read and write operations of SCSI-2: "SCSI Interface 15 performs the distinguishing function during both encryption and decryption. Specifically, when data is being sent from the host computer, encrypted, and written on the tape drive, SCSI Interface 15 distinguishes the 'write' command sent from the host computer from data sent from the host computer. Likewise, when data is being read from the tape drive, decrypted, and sent to the host computer, SCSI Interface 15 distinguishes the 'read' command sent from the host computer from data." (Appx 28, Appx519:8-

[2] In arguing that "SCSI command is sent only during the COMMAND phase and user data is sent only during the DATA phase" of a READ(6)/WRITE(6) operation, Seagate also cited portions of Dr. Conte's deposition but selectively omitted testimony explaining that non-user data that ***would not need to be encrypted*** is also transferred during the DATA phase. (Appx359 (citing, *e.g.* Appx2156:2-2157:21, but leaving out Appx2155:19-2156:1)). In other words, Dr. Conte's position was that even under the READ(6)/WRITE(6) theory, no distinguishing occurs because both user data that needs to be encrypted and non-user data that does not need to be encrypted is transferred during the DATA phase. (*See*, *e.g.*, Appx2148:14-2149:23, Appx2153:15-19, Appx2155:19-2156:1).

520:19, Appx548:10-14).

The declaration never explained how the C/D wire operated with READ(6) and WRITE(6) to distinguish between data signals and control/command signals in the data stream or otherwise. (*Compare* Appx359 *with* Appx1134). Accordingly, even Seagate admitted that Dr. Long's discussion of this belated new theory was "incomplete." (Appx547:10-22).

In addition to lacking substantial evidence that the READ(6)/WRITE(6) theory worked as its attorneys alleged it did, nothing in *Nolan* describes how *Nolan*'s microprocessor decides what to encrypt or decrypt, and there is no concept of, or even mention of the need for, any "data stream interceptor" in the *Nolan* device. *Nolan* fails to suggest, for example, the function of distinguishing command/control signals from data signals, or that command/control signals should be passed through while data signals should be encrypted or decrypted; instead, it merely states that the microprocessor "ascertains whether any transfer of encrypted data is required." (Appx581:23-25). *See also* (Appx291, Appx304-305, Appx568-69 col.4:50-5:17).

Importantly, there is no disclosure of any "input" from the non-existent data stream interceptor that identifies to the microprocessor whether the incoming data stream comprises command/control signals or data. (Appx320-29, Appx527-28). Seagate's expert, Dr. Long, instead states that there is a connection between the

SCSI interface and the microprocessor, and that the microprocessor receives input in the form of commands ***from the host computer*** through the SCSI interface. (Appx325, Appx1134, Appx1139). Unlike the ’995 Patented invention, *Nolan* thus depends on some undisclosed *external* input from the host computer to decide whether to encrypt data, rather than input from a self-contained data stream interceptor. (Appx325-27, Appx581:5-9, 14-18). Even under Seagate’s theory, *Nolan’s* non-transparent device is not only dependent on this external host computer input, but dependent on an attached tape drive to store the encryption key, which it must read before encrypting data. (Appx320-27, Appx581:5-9, 14-18).

In sum, unlike the ’995 patented invention, which has an internal and self-contained data stream interceptor that transparently distinguishes between command/control and data, *Nolan* describes a device significantly dependent on the host computer and storage drive. (Appx581:5-9, 14-18).

It is clear that *Nolan* cannot distinguish between command/control and data signals, as evident by Seagate’s reliance on its READ(6)/WRITE(6) theory. (Appx359). These are the only two instances out of numerous SCSI-2 commands (Appx702, Appx774, Appx843), where Seagate alleges the C/D wire might be used to indicate whether user data or control/command signals is on the data bus. (Appx312-19). Assuming arguendo and accepting that READ(6)/WRITE(6) can

be so used, the C/D wire still does not perform the function of "distinguishing" any more than a broken clock that happens to be "right" twice a day, can actually tell time. *Id*. Nothing in *Nolan* or the SCSI-2 standard discloses the use of voltages on the C/D wire as a way to provide a distinguishing input to the main controller, nor would one expect there to be, since it can only be used as an indicator for two of the many other commands. (Appx313-15, Appx521-22). Rather, even under Seagate's interpretation of Nolan, encryption instructions must come from the host computer. (Appx366-67, Appx581:14-82:8, Appx1139-40).

Because the Board erred in crediting Seagate's belated READ(6)/WRITE(6) theory of obviousness even though there was no substantial evidence to support it, its obviousness determination should be reversed. (Appx29).

3. The Combination of *Nolan* and the SCSI-2 Standard Does Not Teach or Suggest the Requisite Data Stream Interceptor for Distinguishing Signals "In the Data Stream"

Nothing in the combination of *Nolan* with the SCSI-2 Specification discloses any "distinguishing" of signals "***in the data stream"***—as required by the Board's construction of "data stream interceptor." (Appx11, Appx260, Appx308-12, Appx516-17). As set forth above, even under Seagate's theory, Nolan's microprocessor encrypts based on input from the host computer, instead of input from an evaluation of the data stream. (Appx366-67).

Under both of Seagate's theories, before a signal even enters the data stream

going into the cryptographic device, the decision as to whether the signal is a data signal or a command signal is already predetermined by the host computer, so no "distinguishing" is performed "in the data stream." (Appx308-12, Appx508:22-509:12, Appx516-17). Assuming arguendo that Seagate is correct that a high/low voltage in the C/D wire is a reliable indicator of whether command/control or data signals are in the bus, nothing in Nolan or SCSI-2 teaches that this results in any input to the main controller or that such input is used by the main controller for determining encryption or pass-through. (Appx527-30). As Seagate's expert, Dr. Long, also admitted, SCSI data transfers take place ***within*** specific "Information Transfer Phases." (Appx1116-17). While a device is in a particular "Information Transfer Phase," ***only one*** of the COMMAND, STATUS, MESSAGE, or DATA ***phases*** may be invoked on the SCSI Interface 15 data bus at a given time. (Appx307-08, Appx659). Thus, under Seagate's theories, if the Information Transfer Phase is in a COMMAND phase, only command signals are transferred; if it is in a DATA phase, only data signals are transferred. (Appx307-12). No "distinguishing" of signals ***in the data stream*** occurs because, once the Information Transfer Phase is set outside the cryptographic device, only one type of signal is transmitted. (Appx307-308).

Seagate, nonetheless, attempted to argue otherwise[3] using an analogy to describe the "distinguishing" function: "[If] I say, I want tea, and because I said I want tea, I get tea, and then I say, okay, now I want coffee, because I said I want coffee, I get coffee. Anyone would say that I just distinguished between coffee and tea." (Appx489:16-22). In other words, Seagate argues the *Nolan* device in combination with SCSI-2 distinguishes between command/control and data signals because there is a distinction between coffee and tea.

However, the existence of tea or coffee as distinct drinks is not "distinguishing" in the context of the ’995 Patent. (Appx515:10-24). Rather, the claims require observing and *making* a determination or identification between two items—the data stream interceptor must "distinguish ***between*** the command or control signals ***in the data stream*** from the data signals," and the result of that identification is an input used by the main controller to determine whether

[3] This was attorney argument only; it was not in Dr. Long's declaration or deposition transcript. Because the Board did not evaluate Dr. Long's live testimony, any determinations of witness credibility are entitled to no deference. *See* 37 C.F.R. 42.53(a); *Streck, Inc. v. Research & Diagnostic Sys.*, 659 F. 3d 1186, 1191 (Fed. Cir. 2011) (finding Board's reliance on sworn statements did not allow for live and accurate credibility assessments). The failure to scrutinize Dr. Long's credibility is significant given Dr. Long's extensive history with Seagate and his pecuniary interest in the outcome of the IPR. (Appx302-303).

incoming data would be encrypted or passed through.[4] (Appx11, Appx260, Appx311-12, Appx569:52-59).

Certainly, "distinguishing" in advance or by the host computer is not what is claimed; the distinguishing of signals must be done by the data stream interceptor while the data is being transmitted over the SCSI bus, so that its distinguishing input is used by the main controller. (Appx306-311, Appx516:12-518:14). Or, using Seagate's analogy correctly, the "distinguishing" requires that someone taste the stream of liquid and make a determination whether it is coffee or tea.[5] (Appx515:10-24).

Thus, the Board should have rejected both Seagate's C/D wire and READ(6)/WRITE(6) theories because (1) there is no evidence the C/D wire is used to evaluate the incoming data stream to distinguish whether it contains command/control signals or data signals; and (2) there is no evidence that any

---

[4] Seagate alleged it would have been "patently obvious" from *Nolan* to determine whether to encrypt based on the SCSI command sent to the microprocessor, but neither Seagate nor Dr. Long were able to provide a single prior art reference showing this operation. Instead, the references relied upon by Seagate showed that special encryption activation commands, (Appx1065), or user input, (Appx1079), were the common approaches at the time. (Appx2500-01).

[5] While the Board never construed "distinguish," its plain and ordinary meaning requires an act of discrimination. *See Distinguish*, Random House Webster's Unabridged Dictionary (2d. ed. 2001) (defining "distinguish" as "to mark off as different," "to indicate or show a difference," "to set apart as different," "to separate into classes").

distinguishing input is provided to the main controller. These theories stand ***contrary to the Board's own construction of "data stream interceptor,"*** which required that structure to "distinguish the command or control signals ***in the data stream*** from the data signals." (Appx11, Appx253-54, Appx306-12).

4. The Board Erred in Using the '995 Patent as a Roadmap for Assembling Prior Art Elements

That one could even read a data stream interceptor function based on what is disclosed in the SCSI-2 standard is without evidentiary basis absent the improper use of the '995 Patent itself as a roadmap. (Appx523:12-24:14). Nothing in that standard or *Nolan* suggests the need for the cryptographic device to distinguish between command/control and data signals and provide that input to the main controller, let alone construct the '995 Patent's data stream interceptor. As explained above, according to Seagate, *Nolan* "discloses that commands originate from host computer 12." (Appx366-67, Appx1139-40). As such, there would be no need for SCSI Interface 15 to do any "distinguishing," and Dr. Long, in fact, describes that device in terms of a pass-through function (the host computer's commands "then must pass through SCSI Interface 15."). *Id*. Indeed, all *Nolan* discloses about data transfer is that "all data transferred to or from the tape drive passes through the apparatus 10 and can be encrypted or decrypted as required" and that the SCSI Interface 15 can "transfer data to or from the host memory buffer 18 or a target memory buffer 19." (Appx579-80). None of this teaches or suggests

the need for an internal data stream interceptor "that distinguishes between command/control and data signal transfers" as taught and claimed by the '995 Patent, let alone how or why one would put together such a device function when the "commands originate from [the] host computer." (Appx1139-40). That Seagate resorted to citing only two of the many SCSI commands as proof that the C/D wire voltage can indicate whether data or command/control signals are flowing over the data bus only serves to demonstrate Seagate and the Board's use of the '995 Patent as a blueprint. (Appx523:12-24:14).

Nor does the SCSI-2 standard suggest the need for a data stream interceptor internal to the hardware encryption device, as there is no mention at all of an encryption device sitting between a host computer and a hard disk, much less a data stream interceptor (that distinguishes data signals from command/control signals in a data stream for use as input for a main controller to decide what signals should be encrypted). (Appx2396 at 136:9-12).

The Board thus erred in finding obviousness because there was no motivation to combine *Nolan* with the SCSI-2 Standard to come up with the data stream interceptor of the '995 Patent. (Appx221). While Seagate incorrectly asserts that someone ***could*** choose to use READ/WRITE operations of the SCSI-2 standard to build the data stream interceptor of the '995 Patent (which did not exist in either reference and, even according to Seagate's argument, could only work

with READ(6) and WRITE(6) commands), nothing in *Nolan* or the SCSI-2 standard teaches how or even why one ***would*** accomplish that, or suggest the need for such a functional element, except by using the '995 Patent itself as a guide. (Appx359).

It is well-settled, however, that it is improper as a matter of law to use the patent in this manner as a "roadmap" to find obviousness, let alone to construct a missing element (like the data stream interceptor) not disclosed in the prior art. *See InTouch Techs., Inc. v. VGo Commc'ns, Inc.*, 751 F.3d 1327, 1351-52 (Fed. Cir. 2014) (dismissing expert's "belief that one of ordinary skill in the art could combine these references, not that they would have been motivated to do so," and finding impermissible hindsight bias where technical expert relied on asserted patent itself as roadmap for piecing together a "jigsaw puzzle"); *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012) ("[T]he expert's testimony on obviousness was essentially a conclusory statement that a person of ordinary skill in the art would have known, based on the 'modular' nature of the claimed components, how to combine any of a number of references to achieve the claimed inventions. This is not sufficient and is fraught with hindsight bias.").

5. Enova Did Not Have a Fair Opportunity to Respond in Briefing or in the Oral Hearing to Seagate's Belated New Obviousness Theory

The AIA requires that IPR petitions "identif[y]…with particularity…the grounds on which the challenge to each claim is based." 35 U.S.C. § 312(a)(3). As petitioners must set out all of their asserted grounds in their petitions, and patent owners are correspondingly constrained by the contents of their Response, Seagate should have been, under the Board's own rules and authority, foreclosed from raising new arguments in its Reply. *See* 37 C.F.R. § 42.23(b) ("A reply may only respond to arguments raised in the corresponding opposition or patent owner response."); *see also* Trial Practice Guide, 77 Fed. Reg. 78767 ("[A] reply that raises a new issue or belatedly presents evidence will not be considered.")

In similar circumstances, the Court has found waiver of arguments raised for the first time in a reply. *See Novosteel SA v. U.S.*, 284 F.3d 1261, 1274 (Fed. Cir. 2002) ("[R]eply briefs reply to arguments made in the response brief—they do not provide the moving party with a new opportunity to present yet another issue for the court's consideration….As a matter of litigation fairness and procedure, then, we must treat this argument as waived."). By allowing Seagate's new READ(6)/WRITE(6) theory to be raised in a Reply Brief, the Board deprived Enova of a meaningful opportunity to respond, as Enova was allowed no further briefing, and at the Oral Hearing was presumptively constrained to the arguments

in its written Response. *See, e.g.*, *Rambus Inc. v. Rea*, 731 F.3d 1248, 1256 (Fed. Cir. 2013) (Board committed reversible error by adopting a new motivation to combine to which the patent owner did not have a fair opportunity to respond).

C. THE BOARD IMPROPERLY DISMISSED OBJECTIVE EVIDENCE OF NON-OBVIOUSNESS

No substantial evidence supported a prima facie case of obviousness, but even if it did, Enova rebutted this evidence with overwhelming evidence of non-obviousness, and the Board erred in systematically dismissing all such evidence for lack of nexus.

1. Objective Evidence of Non-Obviousness, When Present, Must Be Considered

If a patent challenger establishes a prima facie case of obviousness, a patent owner may come forward with objective evidence of non-obviousness to rebut the prima facie challenge. *Cable Elec. Prods. Inc. v. Genmark, Inc.*, 770 F.2d 1015, 1022 (Fed. Cir. 1985). However, this does not "shift the burden of persuasion," because the ultimate burden of proving unpatentability remains with the petitioner. *Id.*; *see also Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015) (endorsing burden shifting framework in IPRs).

Objective evidence "can establish that an invention appearing to have been obvious in light of the prior art was not" and "may be the most probative and cogent evidence in the record." *Transocean Offshore Deepwater Drilling, Inc. v.*

Maersk Drilling USA, Inc., 699 F.3d 1340, 1349 (Fed. Cir. 2012). These considerations are sometimes referred to as "secondary," not because of diminished importance, but because they often come later (or secondary) in time. *Truswall Sys. Corp. v. Hydro-Air Eng'g, Inc.*, 813 F.2d 1207, 1212 (Fed. Cir. 1987).

When present, objective evidence of non-obviousness must always be considered to guard against hindsight bias. *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1079 (Fed. Cir. 2012). "Just as it is legal error…to fail to consider relevant evidence going to secondary considerations, it may be legal error…to presuppose that all evidence relating to secondary considerations…cannot be of sufficient probative value to elevate the subject matter of the claimed invention to the level of patentable invention." *Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 281, 306 (Fed. Cir. 1985).

Objective evidence of non-obviousness may include commercial success, industry praise, copying, and licensing. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1996). Here, despite strong evidence of non-obviousness tied to the '995 Patent, the Board nonetheless improperly dismissed such evidence—not once—but twice. First, the Board instituted the IPR without considering any objective evidence. (Appx269-70). Second, in its Final Written Decision, the Board

dismissed Enova's evidence of non-obviousness based on an incorrect, and impossibly high standard requiring that the objective evidence explicitly recite claim terms for there to be a nexus with the patent. (Appx42-55). Worse still, the Board rejected Enova's objective evidence even though Seagate offered no counterevidence to rebut Enova's prima facie case of nexus. (Appx337, Appx370-71).

2. At the Institution Stage, the Board Summarily and Erroneously Dismissed All Objective Evidence of Non-obviousness

In finding a "reasonable likelihood" of obviousness, the Board's Institution Decision summarily dismissed all evidence of non-obviousness proffered by Enova, (Appx241-44), stating the record was "incomplete," the evidence was entitled to "little weight," and that evidence of secondary considerations had "no bearing on the legal issue of obviousness," (Appx269-70). However, the PTO should have considered all evidence of non-obviousness and "avoid[ed] giving evidence no weight, except in rare circumstances." MPEP § 2145 (citing *In re Soni*, 54 F.3d 746, 750 (Fed. Cir. 1995)). Here, Enova's Preliminary Response showed that others, including Seagate and Initio, copied the patented technology instead of creating non-infringing alternative solutions to meet the need met by the patented technology. (Appx241-44). Enova also showed that commercial success and industry praise were tied directly to the merits and benefits of the patented invention because the sole purpose of Enova's acclaimed products was their ability

to provide the patented hardware encryption. *Id.*

The Board thus erred in failing to address this objective evidence before finding a "reasonable likelihood" of obviousness. *See Lindemann Maschinenfabrik v. Am. Hoist & Derrick*, 730 F. 2d 1452, 1461 (Fed. Cir. 1984) ("[H]aving concluded that the claimed invention would have been obvious from the prior art, the court looked only to see whether the showing of commercial success was so overwhelming as to overcome that conclusion. That was error. All evidence must be considered before a conclusion on obviousness is reached."); *Apple Inc. v. ITC*, 725 F.3d 1356, 1365 (Fed. Cir. 2013) (holding failure to weigh secondary considerations may constitute reversible error).

This dismissive treatment of Enova's evidence betrays a broader problem—that the potential for hindsight bias is even greater in the IPR context than in district court litigation. Because patent claims in IPRs are construed under the BRI standard, rather than the "plain and ordinary meaning" standard in district courts, the broader claim scope can allow more prior art to be considered, widening the potential for hindsight bias. Objective considerations thus provide a crucial counterbalance in this context and can prevent the Board from "develop[ing] a hunch that the claimed invention was obvious, and then construct[ing] a selective version of the facts that confirms that hunch." *Cyclobenzaprine*, 676 F.3d at 1079 ("[Fact-finders can] unconsciously let knowledge of the invention bias their

conclusion concerning whether the invention was obvious in the first instance.”).

Here, the danger of hindsight bias was compounded because the same three-judge panel that made the decision to institute, (Appx247), conducted the later trial (Appx1). By failing to consider objective evidence at the institution stage, and then justifying its initial “hunch” by again dismissing Enova’s evidence of non-obviousness at the hearing stage, the panel’s unguarded hindsight bias at the institution stage[6] made the final decision more fait accompli than a de novo[7] determination.[8]

3. Commercial Success

At the hearing stage, Enova provided significant evidence that commercial

---

[6] Patent holders cannot challenge an erroneous decision to institute an IPR because that decision is deemed “final and unappealable” under 35 U.S.C. § 314(d). *Cuozzo*, 778 F. 3d at 1282. While *Cuozzo* is pending Supreme Court review, Enova reserves the right to argue that the Board’s Institution Decision should be reviewable because its unguarded hindsight bias at that stage infected the same panel’s downstream final decision.

[7] Under 35 U.S.C. 316(c), the Board is supposed to conduct an independent trial on the merits.

[8] As a result of this process, the Board has consistently dismissed objective evidence, no matter how strong. Of 3,010 Board decisions surveyed, 343 decisions mentioned objective evidence of non-obviousness. *See* Kevin Moran, *A Review of PTAB Cases Involving Secondary Considerations*, *available at* http://www.law360.com/articles/685235/a-review-of-ptab-cases-involving-secondary-considerations (*last accessed* Apr. 18, 2016). But in nearly three years of IPR proceedings under the AIA, patentees have prevailed in ***only two cases*** based on a showing of objective evidence. *Id.*

success was readily apparent from the success of Enova's products as well as Seagate's infringing products. (Appx339-343). For example, Seagate's chief technologist, Dr. Robert Thibadeau, specifically sought out Enova's products to incorporate into its hard drives. (Appx340, Appx2328-30). Recognizing the merits of the invention, a Seagate presentation touted full-disk encryption as a key benefit of Seagate's Momentus product because, among other benefits, there is a "huge bandwidth advantage" (i.e, full-disk encryption does not compromise the system performance), the cryptographic processing is "secret" and "unobservable" (i.e., transparent), and full-disk encryption offered real "value." (Appx340, Appx2340-51). In advertising, Seagate touted its drives as featuring "Hardware-Based Full Disc Encryption (FDE)," a key differentiator among competitors, and described the merits of "[s]trong, transparent hardware-based data protection that prevents unauthorized access to data on lost or stolen laptops." (Appx341, Appx2352) (*see also* Appx2326-39) (praising Enova-enabled encryption as "transparent to the user")); *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573, 1579 (Fed. Cir. 1997) ("The prominence of the patented technology in…advertising creates an inference that links the…invention to this success.").

Indeed, in 2011, Seagate announced it had "shipped more than 1 million self-encrypting laptop and enterprise hard drives" and that "[s]ales of the Seagate® hard drives with built-in encryption continue to surge as more computer makers

offer the drives to protect against unauthorized access to sensitive data, more independent software vendors team up with Seagate…, and more drives win U.S. government certifications." (Appx343, Appx2354-55). As compared with prior art hard drives, shipments of Seagate's Enova-enabled hard drives "have tripled over the past two quarters, while [shipments of self-encrypting laptop drives] have doubled in each of the past three years." (Appx2355).

Seagate further understood the significance of Enova's invention in view of the demands of the market, explaining that because mobile professionals are "demanding stronger, easier to use encryption solutions to protect their sensitive information…[d]rive manufacturers such as Seagate that can deliver stronger security and higher capacity…will be in the sweet spot of market demand for notebooks." (Appx340, Appx2358); *see also Transocean*, 699 F.3d at 1350 (crediting commercial success where there was specific demand for the product and where product became industry standard).

The Board, nonetheless, rejected all evidence of commercial success for lack of nexus, finding Enova had failed to prove the "sales were a direct result of the unique characteristics of the invention, and not a result of economic and commercial factors unrelated to the quality of the patented subject matter." (Appx52-53). The Board also found Enova had failed to provide "any economic analysis" or evidence of the size of the hard drive market to compare Seagate's

sales. (Appx53-54). These findings were erroneous.

For objective evidence to be relevant, there need only be a connection, or "nexus" between the objective evidence and the claimed invention. *Demaco v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988). "Nexus" requires only that a factually and legally sufficient connection exist between the successes of the claimed invention and the claimed invention itself, such that the evidence is of probative value in the determination of non-obviousness. *Id*.

In *Crocs, Inc. v. ITC,* 598 F.3d 1294, 1310-11 (Fed. Cir. 2010), this Court affirmed the long-standing rule that "[a] prima facie case of nexus is made when the patentee shows both that there is commercial success, and that the product that is commercially successful is the invention disclosed and claimed in the patent." Once the presumption is established, "the burden of coming forward with evidence in rebuttal shifts to the challenger." *J.T. Eaton & Co. v. Atl. Paste & Glue Co.*, 106 F.3d 1563, 1571 (Fed. Cir. 1997). The challenger may rebut the presumption by producing evidence "attributing these secondary considerations to causes other than the claimed invention" sufficient to "make a convincing case that those [other factors] indeed were the likely cause of the success." *Crocs*, 598 F.3d at 1311.

As demonstrated above and further below, Enova provided substantial evidence, including Seagate's own statements touting features and benefits of the patented technology, showing that the commercial success of its products was tied

to the claimed invention, (Appx336-45), while Seagate offered no counterevidence despite bearing the burden on unpatentability. (Appx370-71). This should have been fatal to Seagate, but the Board erred in transforming Seagate's burden of providing counterevidence into an additional burden on Enova.

a. Enova Offered Substantial Evidence of Nexus Between Its Objective Evidence of Non-Obviousness and the Claimed Invention

Commercial success need only be "reasonably commensurate with the scope of the claims." *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011). Here, Enova's ASICs are just that, Application *Specific* Integrated Circuits—chips designed to carry out a specific task, in this case, enabling hardware-based full disk encryption as described in the '995 Patent. (Appx2494). The '995 Patent itself stated that "("Cryptographic device 32 may be integrated in ASIC chip form."), (Appx568 col.4:6-8). Indeed, any commercial success or industry praise garnered by Enova's X-Wall Products was entirely attributable to the claimed inventions of the '995 Patent, as Enova does not sell non-encryption ASICs that do not embody the '995 Patent. (Appx2493).

Enova's expert, Dr. Conte, showed how each Enova product completely embodied the claimed invention. (Appx2493-2503) (discussing X-Wall SE, CO, MX, FX and Enigma products).

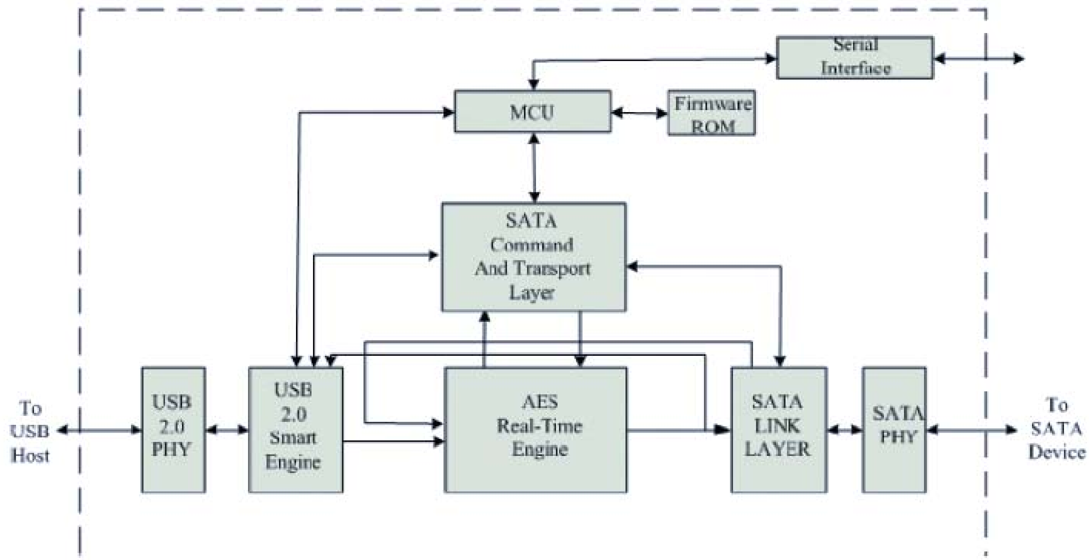


Figure 1 -- The Functional Block of *X-Wall FX*

For example, with regard to the X-Wall FX ASIC, Dr. Conte provided the block diagram above and attested that the X-Wall FX ASIC had a data stream interceptor which operated according to the ’995 Patent: “The X-Wall FX includes a host-side USB controller which intercepts USB signals sent from the Host.” (Appx2496-97). He also showed that the X-Wall FX ASIC had a main controller and cryptographic engine: “Under control of the built-in microcontroller (MCU, above) USB data streams are intercepted and sent to the AES real-time engine, which transparently encrypts them….USB command and control signals bypass the AES engine and are translated into SATA commands, which are sent to the SATA device.” *Id*.

Enova’s Products were expressly marked with only the ’995 Patent and at most two other (related) patents, as shown below.

(Appx2494-95). If patent marking is sufficient notice to trigger damages and could provide the basis of a false marking claim, *see* 35 U.S.C. §§ 287, 292, it should be sufficient evidence that Enova's products are coextensive with the merits of the '995 Patent—especially where Seagate has provided no counterevidence that the X-Wall products were falsely marked, or that they did not fully embody the '995 Patent.

b. In Finding No Nexus, the Board Erred in Relying Only on Seagate's Attorney Argument and Conjecture

Once the patentee demonstrates a prima facie nexus, the burden of coming forward with evidence in rebuttal shifts to the challenger. *Omron Oilfield & Marine, Inc. v. MD/Totco*, IPR2013-00265, Paper 11, at 14 (P.T.A.B. Oct. 31, 2013). Against the weight of Enova's evidence, Seagate submitted nothing but attorney argument and conjecture, even though it is "the task of the challenger to adduce evidence to show that the commercial success was due to extraneous factors other than the patented invention, such as advertising, superior workmanship, etc.…'[A]rgument' and 'conjecture' are insufficient." *Demaco*, 851

F.2d at 1393; *see also Omron Oilfield*, at 14-15 (denying institution of IPR because evidence of commercial success was unrebutted); (Appx337, Appx370-71).

In its Reply, Seagate spent only half a page on secondary considerations, relying on bare attorney argument to summarily conclude that Enova failed "to show how each claim element is found in these products, much less provides a nexus between the merits of the '995 Patent's claimed invention and the products, licenses, and stipulation." (Appx337, Appx370-71). This assertion is not supported by a counter-declaration and is objectively false. As discussed above, Dr. Conte's Declaration established how each claim element was found in each of Enova's X-Wall products. (Appx2494-99). In fact, Seagate's expert admitted at deposition that Seagate did not "provide [him] with any information regarding secondary considerations," that he did not do any research about secondary considerations, and that he "wasn't asked to." (Appx2402; *see* Appx1175 (expert failing to consider secondary considerations in analysis)). There was no counter-declaration that the X-Wall products were falsely marked, or that any X-Wall products failed to practice the '995 Patent. There was no evidence suggesting that commercial success was instead based on non-patented factors, such as superior branding or marketing prowess. And, there was no evidence that sales were driven

by any non-patented feature—nor could there be, since the X-Wall ASICs were single-purpose items, in contrast with multi-featured products like smartphones.[9]

Rather than submit counterevidence, Seagate filed an improper Motion to Exclude Enova's objective evidence of non-obviousness in what amounted to an end-run around the Board's page limitations on substantive briefing. (Appx373-89; *see* Appx545 (judge noting "it's unusual to see that type of argument presented in a motion to exclude" because "[i]t's usually presented somewhere in the brief and I know you were constrained somewhat by your page limits"); Office Patent Trial Practice Guide, 77 Fed. Reg. at 48,767 ("[A motion to exclude] may not be used to challenge the sufficiency of the evidence to prove a particular fact.")). The Board then adopted the arguments in Seagate's Motion to Exclude as its own, sub silencio acting upon a motion that the Board itself had declared moot and that should not have been considered at all. (Appx56) (Board declaring Motion to Exclude moot and stating disingenuously that "[w]e do not rely on [the Motion to Exclude in] rendering this Final Written Decision").

---

[9] Indeed, unlike in *Microsoft Corp. v. Proxyconn, Inc.*, where the patented feature was "itself not a product but one feature of a complex software product," the '995 patented invention is the very product embodied in Enova's X-Wall ASICs. IPR2013-00026, Paper No. 32, at 5 (PTAB March 8, 2013) ("Where, as here, the patent is said to cover a feature or component of a product, the patent owner has the additional burden of showing that the commercial success derives from the feature.")

It was thus error for the Board to accord no weight to Enova's evidence, while crediting Seagate's attorney arguments. In *Crocs*, the patent challenger similarly offered no evidence to rebut the patentee's prima facie case of commercial success. *Crocs*, 589 F. 3d at 1311. As a result of the challenger's failure to show that market forces instead were the likely cause of the success, the Court credited the patent owner's proof of non-obviousness. *Id*. The Board should have acted similarly here.

c. The Board Erred in Requiring an Economic Analysis to Show Commercial Success

The Board also found that Enova had failed to provide "any economic analysis" or evidence of the size of the hard drive market to compare Seagate's sales. (Appx53-54). Having shown nexus through other means, however, there was no need for Enova to have provided such analysis or evidence. *Demaco*, 851 F.2d at 1392.

4. Industry Praise

Enova's evidence of industry praise also supported non-obviousness. (Appx338-39, Appx44-52); *see Transocean*, 699 F.3d at 1351-52 (finding substantial evidence supporting non-obviousness where industry praise cited features and benefits of patented invention)). As discussed above, Dr. Conte's unrebutted testimony was that Enova's X-Wall line of products, including the X-Wall SE and X-Wall MX products all practice the claimed invention of the '995

Patent. (Appx337-38, Appx2494-99). The industry praise directed at these practicing products was thus conclusively attributable to the ’995 Patent.

For example, Enova’s XWall MX won a 2012 Business World Golden Bridge Award in the Encryption Solutions Innovations category. (Appx339, Appx2496, Appx2522-27). Moreover, Enova’s Enigma I, a USB device that Dr. Conte testified is “totally transparent” and fully embodies the ’995 Patent, (Appx2497-2500, Appx2597-98), was awarded PC Magazine’s 2012 Editor’s Choice Award and an “Excellent” rating. PC Magazine praised Enigma’s “[s]imple, seamless full-disk encryption for any USB mass storage device.” (Appx338-39, Appx2497-2500, Appx2514-18).

The Board nonetheless rejected Enova’s unrebutted evidence of industry praise as lacking nexus because it believed (1) the praise was not “due to specific elements that are recited in the challenged claims;” and (2) even were the praise attributable to claimed elements, these elements already existed in the prior art. (Appx44-52). These impossible standards for nexus are not only unsupported by case law but are refuted by the record.

a. The Board Erroneously Dismissed Enova’s Evidence of Industry Praise Based on an Incorrect, and Impossibly High Standard Requiring that Objective Evidence Explicitly Recite Claim Terms to Establish Nexus

Despite unrebutted evidence that the sole purpose of Enova’s acclaimed products was to practice the claimed invention, the Board dismissed the evidence

of industry praise and commercial success as not having sufficient nexus because it was not "due to specific elements that are recited in the challenged claims." (Appx44-45).

This is an impossible standard to meet, as industry praise is rarely directed at specific claim elements. The Board's standard is furthermore entirely unsupported by case law, as objective evidence need only be "reasonably commensurate with the scope of the claims." *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011); *Demaco*, 851 F.2d at 1392. Enova's unrebutted proof that the praise-earning X-Wall products practiced the '995 Patent was more than enough. As in *Transocean*, Enova's evidence linked both the industry praise regarding the security and ease-of-use provided by Enova's products directly to the claimed "transparent" and seamless encryption features. *See supra* Section C.3.a; *Transocean*, 699 F.3d 1351-52 ("Transocean's evidence…links both the industry praise and the unexpected efficiency gains directly to the claimed dual-activity feature.").

b. The Board Erroneously Dismissed Enova's Evidence of Industry Praise Because Such Evidence Was Allegedly Disclosed in Prior Art

The Board further found no nexus with the claimed invention because, in its view, the "transparently" encrypting feature and the "hardware-based encryption" discussed in the objective evidence was already disclosed in *Nolan* and SCSI-2.

(Appx47, Appx51). This finding lacks substantial evidence and is legally erroneous.

First, *Nolan* does not, in fact, transparently encrypt data because, as discussed in Section D.2.c below, *Nolan* requires intervention by the user and the interaction of the cryptographic device with the storage media in order to retrieve the encryption key. Even assuming *Nolan* did transparently encrypt, the Board's dismissal of Enova's objective evidence based on this single feature would have been legal error. *See Rambus*, 731 F.3d at 1257 (determining that Board erroneously disregarded evidence of non-obviousness as lacking nexus because a single claimed functionality was disclosed in the prior art).

Second, the Board's backwards logic is legally incorrect. By definition, every prima facie determination of obviousness will involve prior art; but, under the Board's logic, this prior art will always preclude a finding of nexus and improperly obviate the need to conduct any analysis of objective evidence. *In re Cyclobenzaprine*, 676 F.3d at 1079; *Transocean*, 699 F.3d at 1349.

The Board relied on *Tokai Corp. v. Easton Enterprises, Inc.*, 632 F.3d 1358, 1369-70 (Fed. Cir. 2011), for the proposition that "[i]f [secondary considerations are] due to an element in the prior art, no nexus exists."), but that reliance is misplaced. *Tokai* did not hold as a matter of law that there can be no nexus to commercial success where components of the patented invention were available in

the prior art.[10] Rather, the Court in *Tokai* decided as a factual matter that there was no nexus because in that case the product as a whole—utility lighters with child-safe features—were available in the prior art, such that it could not be said that proof of sales of the patented lighters with comparable safety features had a nexus to the patented, particular of effecting lighter safety. *Id.* On appeal, the patentee conceded that such child-safe lighters were already on the market, and the Court found no reason to disagree. Moreover, in *Tokai*, the objective evidence never referenced the "feature that purportedly distinguishes the claimed inventions from prior art utility lighters." *Id.* at 1370.

By contrast, the industry praise here is expressly directed to the transparent encryption feature of the claimed invention. Furthermore, the situation here is not one where any prior art products existed with similar features, as a whole or otherwise. Unlike the prior art, the '995 Patent enabled full-disk, on-the-fly

---

[10] Neither did the case cited by *Tokai* so hold. *See Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1580 (Fed. Cir. 1983). Like *Tokai*, the cited passage in *Richdel* similarly dealt with a factual finding that the record in that case provided no showing that the patented improvement contributed to the alleged commercial success. There was no analysis at all of secondary considerations in *Richdel* because the court found, contrary to current law, that, "where a patent is obvious, it cannot be saved from invalidity by resorting to secondary factors." *Id*. at 1580; *cf. Transocean Offshore Deepwater v. Maersk Drilling*, 699 F. 3d 1340, 1349-52 (finding a nexus between commercial success and the patented features notwithstanding prima facie obviousness).

automatic encryption with no user intervention and without taxing system resources. There is no evidence that *Nolan* or any other prior art product provided these features. Indeed, as shown above, *Nolan* did not even describe the claimed data stream interceptor. Instead, it worked with a tape drive that required user intervention, relied on commands originating from the host computer, and would tax system resources by requiring the encryption key be accessed from the tape drive before encryption operations could commence. Enova's acclaimed products had a single purpose, such that their commercial success was directly attributable to the patented invention, (*see* Appx2493-2500), unlike the utility lighters in *Tokai*, which had non-patented uses (like providing a flame) apart from the particular way in which they implemented the patented child-safety feature. As Enova's evidence of industry praise was not disclosed in the prior art, the Board's failure to accord any weight to Enova's evidence of industry praise was error—especially where Seagate failed to offer any evidence to rebut Enova's objective evidence. *See supra* Section C.3.b.

5. Copying and Licensing

Here, copying of the patented products—by Seagate and others—points to non-obviousness. *See Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1325 (Fed. Cir. 2004); *Akamai Tech. v. Cable & Wireless Internet Servs.*, 344 F. 3d 1186, 1196-97 (Fed. Cir. 2003).

For example, after first collaborating with Enova to embed Enova's patented X-Wall MX encryption ASICs into its products, Initio Corporation, a competing chip maker, began marketing and selling infringing products. (Appx343-45, Appx2324-25, Appx2599-2600). Initio ultimately entered into a consent judgment, admitting that it had "infringed directly and indirectly, literally or under the doctrine of equivalents, the asserted claims of U.S. Patent No. 7,136,995." (Appx2324-25, Appx2719-21). Initio also began marking its chips with the '995 Patent. (Appx343-45, Appx2714). Initio and its customer, Western Digital, now license the '995 Patent from Enova, (Appx343-45, Appx2679-711)—yet another factor that weighs in favor of non-obviousness. *RCA Corp. v. Data Gen. Corp.*, 701 F. Supp 456, 471 (D. Del. 1988), *aff'd*, 887 F.2d 1056 (Fed. Cir. 1989).

The Board, nevertheless, concluded Initio's consent judgment was not evidence of infringement and lacked nexus because "it is not sufficient that a product or its use merely be within the scope of a claim in order for objective evidence of non-obviousness…to be given substantial weight." (Appx55). This Court, however, has held that copying may be demonstrated by access to and substantial similarity to the patented product as opposed to the patent itself. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1285 (Fed. Cir. 2000). In *Transocean*, the Court overturned a finding of a prima facie case of obviousness partly based on substantial evidence of copying that "showed that

Maersk was aware of Transocean's patents and its drillships embodying the patents while Maersk designed its accused rig," but "Maersk decided to incorporate the claimed dual-activity feature anyway because it believed Transocean's patents were invalid over the prior art." 699 F.3d at 1352.

Here, the evidence of copying is even stronger because, unlike Maersk, which was merely aware of the patents, Seagate and Initio had actual access to the patented product itself. *See Iron Grip Barbell*, 392 F.3d at 1325 (holding that evidence that a copying party had "access to…the patented product (as opposed to the patent)" is sufficient evidence of copying). The Board thus improperly failed to credit Enova's unrebutted evidence by ignoring that both Seagate and Initio were aware of Enova's products and had copied and later sold infringing products having the same functionality as the practicing X-Wall products. (Appx343-45). And though Seagate had an opportunity to do so, (Appx1175), it never disputed that it had access to Enova's patented ASICs, incorporated the ASICs into its products, and continued to sell products incorporating the patented encryption system even after it stopped purchasing from Enova, (Appx2540-42, Appx2556-57, Appx 2559-61, Appx342-43).

Finally, the Board also erred in declining, without justification or prompting by Seagate, to consider licensing evidence, citing its inability to "verify [Enova's] assertions regarding these arguments." (Appx55). While the proffered licenses

were redacted due to confidentiality obligations, the redactions were not such that the Board could not tell that they were licenses between Enova and each of Initio, Western Digital, and Buffalo involving the ‘995 Patent. (Appx541-43, Appx2679-2711, Appx2501-03). Though these licenses were borne out of litigation, *Initio* involved only three patents—the ’995 Patent-at-issue and two other patents in the same family, and at least one of the parties to the litigation and license—Initio—admitted its products infringed the ’995 Patent. (Appx2324-25, Appx2719-21). As Enova made a prima facie showing of nexus that was completely unrebutted by Seagate, the Board erred in not crediting Enova’s evidence of non-obviousness.

D. THE BOARD’S CLAIM CONSTRUCTIONS WERE UNREASONABLY BROAD IN LIGHT OF THE CLAIMS AND SPECIFICATION

In IPRs, claims are to be accorded their broadest reasonable interpretation in light of the specification. *In re Cuozzo Speed Techs, LLC*, 793 F.3d 1268 (Fed. Cir. 2015) (cert. granted). Even if such remains the appropriate standard,[11] the Board incorrectly applied it.

[11] Enova reserves the right to challenge the Board’s use of the BRI standard in the event *Cuozzo* is overturned during the pendency of this appeal. *See id.*

1. The Board's Construction of "Input" is Unreasonably Broad

a. "Input" Must Distinguish the "Incoming Data" for the Main Controller

The parties dispute the construction of "input," which appears in every independent claim of the '995 Patent. Exemplar Claim 9 of the '995 Patent recites a "main controller receiving ***input*** from said … data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through ***based on the received input*** from said … data stream interceptor." (Appx569 col.6:45-52) (emphases added). The data stream interceptor thus distinguishes—makes a determination of—whether the signals in the data stream are command/control signals or data signals, and provides that identification in the form of an input to the main controller. The main controller, in turn, receives the "input from [the] data stream interceptor," and determines whether the incoming data stream is to be "encrypted, decrypted or passed through ***based on*** the received input" from the data stream interceptor. *Id.*

Importantly, the received input must provide the "bas[is]" for the main controller to determine whether the data should be encrypted, decrypted, or passed through. (Appx569 col.6:45-52, Appx2437-40). Enova, as did the *Initio* court, therefore proposed that the construction of "input" be properly constrained by its function: "input distinguishing between command/control and data signal transfers from the data stream interceptor." (Appx14-15, Appx258, Appx296-97,

Appx2321-22). Seagate did not propose a construction for "input." (Appx257-58). The Board, nonetheless, construed "input" as the command/control or data signals themselves, rather than as an identification of the signals as one or the other of command/control or data signals. (Appx14-15, Appx257-58).

As discussed below, by allowing the command/control and data signals themselves to be the "input," the Board's construction improperly read out two important claim terms ("incoming data" and "data stream interceptor") and ignored the requirement that the input must distinguish between command/control and data signals. (Appx14-15, Appx258, Appx296-97, Appx2321-22, Appx569 col.6:45-52, Appx2437-40).

b. The Board's Construction of the Term "Input" Renders the Term "Incoming Data" Superfluous

The Board's construction of "input" as command/control or data signals, gives "input" the same meaning as the term "incoming data," and renders that term superfluous. "[T]he general assumption is that different terms have different meanings." *Symantec Corp. v. Computer Assoc. Int'l, Inc.*, 522 F.3d 1279, 1289 (Fed. Cir. 2008). Here, claim 9 recites a "main controller receiving ***input*** from said…data stream interceptor and determining whether ***incoming data*** would be encrypted…based on the received input." (Appx569 col.6:45-52) (emphases added). The specification itself defines "incoming data" as "includ[ing] command/control and/or data signals." (Appx568 col.4:55-58) ("Main controller

432 ***receives input*** from data stream interceptor 431 and determines whether an ***incoming data stream, which may include command/control and/or data signals***, is to be encrypted, decrypted or passed through unmodified.") (emphases added). Because "incoming data" necessarily encompasses the actual command/control and data signals, the term "input," which is used to provide information about that "incoming data," should not be accorded the same meaning.

c. The Board's Construction of the Term "Input" Reads Out the Term "Data Stream Interceptor"

As made clear by the intrinsic record, the "incoming data" comprises the command/control signals or the data signals themselves, while the "input" is a separate determination made by the data stream interceptor *about* that information—the identification of whether that incoming data in the data stream is a command/control or a data signal. (Appx568 col.4:55-58, Appx569 col.6:45-52). The "input" in turn forms the "bas[is]" for the main controller to determine "whether incoming data would be encrypted, decrypted, or passed through." (Appx569 col.6:45-52). If the "input" were one and the same with the command/control or data signals themselves, the main controller would lack the identification input necessary to determine "whether incoming data should be encrypted, decrypted, or passed through," as it would not have the benefit of the data stream interceptor having "distinguished" between command/control and data signals.

The Board's construction, under which "input" is the command/control and/or data signals themselves, instead requires the main controller to perform the "distinguishing" function, rather than the data stream interceptor. This is contrary to the claims, which require the main controller to "determin[e] whether incoming data would be encrypted, decrypted or passed through ***based on*** the received input." Under the Board's construction, the "input" from the data stream interceptor has no role in distinguishing between command/control and data signals to enable the main controller to determine whether incoming data should be encrypted, decrypted, or passed through. (Appx15, Appx33). Reading out the role of the data stream interceptor is improper. *See, e.g.*, *Lantech, Inc. v. Keip Mach. Co.*, 32 F. 3d 542, 546 (Fed. Cir. 1994) ("All limitations in a claim must be considered meaningful."). The Board's construction is thus overly broad and unreasonable because it conflicts with the claims and the specification and reads out other limitations. *Id.*

d. Enova's Construction of "Input" Is Consistent with the BRI Standard

As shown above, Enova's proposed construction, which was adopted by the court in *Initio*, (Appx2321-22), is also the broadest reasonable interpretation of the claims supported by the specification. (Appx296-97) ("[C]onstruction of this term "requires that 'input' resulting from the 'distinguishing' be sent to and used in some way by the main controller in 'determining") (quotation omitted). This

construction is appropriate, as the claims and specification dictate that the data stream interceptor distinguishes between command/control and data signals and provides that identification as an input for use by the main controller—even under the BRI standard. The BRI standard is not so broad as to allow rewriting the claims to allow the main controller to usurp the "distinguishing" function of the data stream interceptor, rendering that claim element, and the "input" it provides, surplussage.

e. The Board's Failure to Evaluate the District Court's Claim Construction Order Separately Requires Remand

Despite its obligation to do so, the Board did not evaluate the *Initio* court's claim construction. (Appx15, Appx2321-22); *see Allentown Mack Sales & Serv., Inc. v. NLRB*, 522 U.S. 359, 374 (1998); *In re Sang-Su Lee*, 277 F.3d 1338, 1342 (Fed. Cir. 2002) (holding that Board is obligated not only to come to a sound decision, but to fully and particularly set out bases upon which it reached that decision)). Here, the Board stated simply that it was not bound by the *Initio* claim construction. (Appx15). But "[t]he fact that the [B]oard is not generally bound by a previous judicial interpretation of a disputed claim term does not mean…that it has no obligation to acknowledge that interpretation or to assess whether it is consistent with the broadest reasonable construction of the term." *Power Integrations v. Lee*, 797 F.3d 1318, 1326-27 (Fed. Cir. 2015).

In *Power Integrations*, the Court held that the Board erred in failing to

address the district court's previous interpretation of a term: "Given that [patent owner's] principal argument to the Board about the proper interpretation of the term 'coupled' was expressly tied to the district court's claim construction, we think that the Board had an obligation, in these circumstances, to evaluate that construction and to determine whether it was consistent with the broadest reasonable construction of the term." *Id.* As the Board here fell short of its obligation to "set[] out its reasoning in sufficient detail to permit meaningful appellate review," the Board's claim construction determination should be vacated on this ground. *Id.* at 1327.

f. Under a Proper Construction of "Input," Nolan Does Not Render the '995 Patent Obvious

Nolan does not render the '995 Patent obvious because, as discussed above and at the May 11, 2015, Oral Hearing, *Nolan* fails to disclose any input used by the main controller to enable it to determine whether incoming data would be encrypted, decrypted, or passed through. (Appx529-31). The Board overlooked this shortcoming, finding that it sufficed for *Nolan's* microprocessor to receive any kind of incoming data. Instead, the Board expressly relied on its improper construction of "input" to conclude that *Nolan* need not "teach [that] a microprocessor receives input resulting from the distinguishing function performed by the data stream interceptor." (Appx33). As the "input" must result from the distinguishing function of the data stream interceptor, the Court should remand the

Board's claim construction of "input" as overly broad. Under the correct construction, *Nolan* cannot be considered prior art.

2. The Board's Construction of "Transparently" Is Unreasonably Overbroad

a. The Board Used a Dictionary Definition Contrary to the Intrinsic Record

Claim 9 recites "at least one cipher engine adapted to ***transparently encrypt or decrypt*** at least one data stream" between the data generating device and the data storage device. (Appx569 col.6:61-64) (emphasis added). In construing "transparently," the Board ignored the claim language and the specification and sua sponte turned to a single extrinsic reference—the 1997 edition of the Microsoft Computer Dictionary, which defined "transparent" to mean "pertaining to, or characteristic of a device, function, or part of a program that works so smoothly and easily that it is invisible to the user." (Appx255-256, Appx296, Appx2788; *see* Appx13-14). From this, the Board construed "transparently" to mean "functionally invisible"— a term nowhere to be found in the intrinsic record and so abstract and unhelpful that it requires its own construction. (Appx2788; *see* Appx13-14, Appx256-57).

Neither party requested this construction. Enova proposed that "transparently" be construed as "functionally, data transfers appear to be performed directly between the data generating device and data storage device."

(Appx212-13, Appx296, Appx255-57). Enova based this construction on the specification, which teaches that the claimed invention can encrypt/decrypt data "without compromising the overall system performance," such that "from the functional viewpoint" of either device, such data transfers are "performed directly." (Appx568 col.3:30-34). Seagate proposed that "transparently" be construed to mean "without using resources associated with data generating or data storage devices." (Appx79-80, Appx255-57).

The Board dismissed both proposed constructions, explaining only that those constructions were "more restrictive than the claim language, which does not ***recite explicitly*** that data transfers appear to be performed directly between the data generating device and data storage device." (Appx14) (emphasis added); (*see also* Appx256-57). The Board thus appears to have adopted a circular test for claim construction, requiring that the claims themselves "recite explicitly" any proposed construction.

The Board's reasoning, which contravenes the specification, lacks legal basis and is incorrect as a matter of law. Claims should be construed in light of the specification, even under the broadest reasonable interpretation standard. *Microsoft*, 789 F. 3d at 1298 (The Board may not "construe claims during IPR so broadly that its constructions are unreasonable under general claim construction principles."); *Phillips v. AWH Corp.*, 415 F. 3d 1303, 1315 (Fed. Cir. 2002) ("[The

specification] is the single best guide to the meaning of a disputed term." (quotations omitted)). The non-existence of an express definition is not a barrier to proper construction; indeed, such express definitions are rarely present. *Id.* at 1321 (specification need not expressly define a term and may still act as a "dictionary" when it "defines terms by implication").

The Board's construction here mirrors its approach in a previous decision vacated by this Court, *PPC Broadband, Inc. v. Corning Optical Communications*, No. 2015-1364, slip op. at 7-12 (Fed. Cir. Feb. 22, 2016). In *PPC Broadband*, as here, the Board bypassed the intrinsic record and sought out the broadest dictionary definition it could find. *Id*. at 7-9. In so doing, the Board failed to "account for how the claims themselves and the specification inform the ordinarily skilled artisan as to precisely which ordinary definition the patentee was using." *Id*. As a result, the Board arrived at an incorrect and unreasonably broad construction, elevating an extrinsic reference over the patent specification even though the specification "provides strong support for [patentee's] interpretation." *Id*. at 9-12 ("Above all, the broadest reasonable interpretation must be ***reasonable*** in light of the claims and specification.").

b. "Transparently" Refers to Data Transfers "Without Any Intervention by the Cryptographic Device"

The specification explains the term "transparently" from the functional viewpoint of the computer and disk drive: "data transfers are being performed

directly between data generating device and/or data storage device…without any intervention by cryptographic device [which acts as] an invisible data transfer bridge….” (Appx216-217, Appx568 col.3:30-37). The Board's dictionary-based construction to mean “functionally invisible” from a computer user's perspective is thus inconsistent with the patent specification, and wrong. (Appx296, Appx2106:8-23, Appx2448-49).

The Board attempted to cast its user-centric construction as consistent with the specification by pointing to the statement: “[i]n general, the cryptographic device acts as an ***invisible*** data transfer bridge connecting the data generating device and data storage device.” (Appx256). But this use of the word is out of context with the surrounding text and other statements in the specification where the word “invisible” is repeatedly used to refer to a cryptographic device that operates as if “data transfer is being performed directly…without any apparent intervention” by the cryptographic device. (Appx568 col.3:30-33, col3:66-col.4:2, col.4:25-29).

c. Under the Correct Construction, Nolan Does Not Operate “Transparently”

As a result of its flawed construction, the Board found that *Nolan* functions “transparently,” when instead it requires additional input from at least the data storage devices. (Appx581-82, Appx326, Appx334-35). In particular, *Nolan* must store the data encryption key on the tape, and every time it needs to encrypt data, it

must perform additional data transfers between the apparatus and the data storage device to store or retrieve the key. (Appx581) ("This key, which is to be common to all data on the tape, is stored on the tape before any data is written to the tape….[T]he microprocessor reads the common encryption key stored on the tape and stores it in the unit"). Because these additional read/write operations force the data storage device to store and retrieve data not otherwise required if connected directly to the host computer, *Nolan* cannot be said to operate "transparently." *Id*. Furthermore, such additional disk read/write operations "affect overall system performance," contrary to the specification. (Appx562 (Abstract)).

Finally, even under the user perspective construction of the Board, *Nolan* still fails to operate "transparently" because it requires a user to first input a data encryption key into a keypad before it can generate additional cryptographic keys. (Appx326-27, Appx581). This is significant because the specification expressly discourages such manual user intervention: "Worse still, [the prior art] frequently results in compromised overall system performance, and requires manual intervention by users who may become confused and frustrated by the number of requisite interactive steps embedded in the application." (Appx657 col.1:47-51). "[W]hen the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007); *see also In re*

Caldwell, 319 F.2d 254, 256 (C.C.P.A. 1963) (reference teaches away if it leaves the impression that the product would not have the property sought by applicant); *Medichem S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006) ("[A reference teaches away when it suggests] the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant."). As *Nolan* would discourage an applicant "from following the path set out" in the '995 Patent, it cannot create a prima facie case of obviousness.

CONCLUSION

For the foregoing reasons, the Court should reverse, or in the alternative, vacate and remand the Board's obviousness determination with appropriate instructions.

Dated: April 18, 2016

Respectfully submitted,

/s/ *Darryl M. Woo*
DARRYL M. WOO
VINSON & ELKINS LLP

Counsel for Appellant
Enova Technology Corporation

ADDENDUM

ADDENDUM TABLE OF CONTENTS

Trials@uspto.gov
571-272-7822

Paper 47
Entered: September 2, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SEAGATE TECHNOLOGY (US) HOLDINGS, INC. and
SEAGATE TECHNOLOGY LLC,
Petitioner,

v.

ENOVA TECHNOLOGY CORP.,
Patent Owner.

Case IPR2014-00683
Patent 7,136,995 B1

Before MICHAEL R. ZECHER, GEORGIANNA W. BRADEN, and FRANCES L. IPPOLITO, *Administrative Patent Judges.*

IPPOLITO, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Seagate Technology (US) Holdings, Inc. and Seagate Technology LLC (collectively "Petitioner") filed a Corrected Petition ("Pet.") requesting an *inter partes* review of claims 1–15 of U.S. Patent No. 7,136,995 B1 ("the '995 patent"). Paper 4. Enova Technology Corp. ("Patent Owner") timely filed a Preliminary Response ("Prelim. Resp.") to the Petition. Paper 9. Based on these submissions, we instituted trial as to claims 1–15 of the '995 patent on the following proposed grounds of unpatentability:

Reference(s)	Basis	Claim(s) Challenged
Nolan[1] and SCSI-2[2]	§ 103	1–13
Nolan, SCSI-2, and Hamlin[3]	§ 103	14
Nolan, SCSI-2, and Detrick[4]	§ 103	15

Paper 10, 29 ("Dec. to Inst.").

After institution, Patent Owner filed a Patent Owner's Response (Paper 22, "PO Resp."), and Petitioner filed a Reply (Paper 27, "Reply"). In addition, Petitioner filed a Motion to Exclude. Paper 31 ("Pet. Mot. Exclude"). Patent Owner filed an Opposition to Petitioner's Motion to Exclude (Paper 38, "PO Exclude Opp."), and Petitioner filed a Reply (Paper 42, "Pet. Exclude Reply"). Patent Owner filed a Motion to Exclude. Paper 33 ("PO Mot. Exclude"). Petitioner filed an Opposition to Patent Owner's Motion to Exclude (Paper 37, "Pet. Exclude Opp."), and Patent Owner filed

[1] GB Patent App. No. 2,264,373 A, published Aug. 25, 1993 (Ex. 1002, "Nolan").
[2] ANSI, SMALL COMPUTER SYSTEM INTERFACE-2 (ANSI X3.131-1994 (R1999), 1994) (Ex. 1003, "SCSI-2").
[3] US Patent No. 6,735,693 B1, issued May 11, 2004 (Ex. 1004, "Hamlin").
[4] US Patent No. 7,278,016 B1, issued Oct. 2, 2007 (Ex. 1005, "Detrick").

a Reply (Paper 41, "PO Exclude Reply").

Patent Owner also filed a Motion to Seal Exhibits 2042, 2043, and 2044 (Paper 23, "Mot. to Seal"), which is addressed herein.

An oral hearing was conducted on May 11, 2015. A transcript of the oral hearing is included in the record. Paper 46 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This decision is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of claims 1–15. For the reasons discussed below, Petitioner has demonstrated by a preponderance of the evidence that claims 1–15 are unpatentable.

A. Related Proceedings

Petitioner indicates the '995 patent currently is the subject of a related proceeding between the parties in the U.S. District Court for the District of Delaware titled *Enova Tech. Corp. v. Seagate Tech. (US) Holdings, Inc.*, No. 1:13-cv-1011-LPS, which was filed on June 5, 2013. Pet. 1; Paper 7, 2. Petitioner also indicates the '995 patent was the subject of a prior federal district court proceeding in the U.S. District Court for the District of Delaware, No. 1:10-cv-00004-LPS ("*Enova v. WD*"), which closed on March 4, 2013. Pet. 1. Additionally, related U.S. Patent No. 7,900,057 B2 is the subject of an *inter partes* review in Cases IPR2014-01178, IPR2014-01297, and IPR2014-01449.

B. The '995 Patent

The '995 patent describes a cryptographic device that performs encryption/decryption during data transfers between a data generating device and a data storage device. Ex. 1001, 3:22–24. Figure 4 (reproduced below)

depicts schematically the architecture of cryptographic device 43 described in the ’995 patent. *Id.* at 4:30–32.

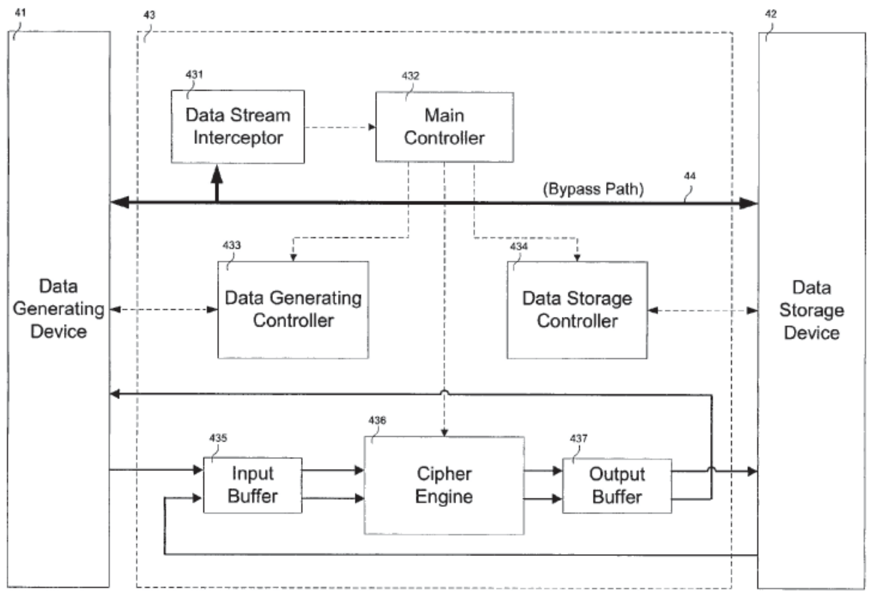


FIG. 4

Figure 4 shows cryptographic device 43 operatively coupled between data generating device 41 and data storage device 42 for use during data transfer. *Id.* at 4:32–35. The ’995 patent indicates that data generating device 41 may be “a desktop/notebook computer, microprocessor . . . or any other device capable of generating data.” *Id.* at 4:35–38. The ’995 patent adds that data storage device 42 may be “a computer hard drive, tape drive . . . magnetic tape . . . or any other device capable of storing data for retrieval purposes.” *Id.* at 4:38–44. Further, cryptographic device 43 is described as adapted to “perform transparently data encryption and decryption during data transfers between data generating device 41 and data storage device 42 with no impact on overall system performance.” *Id.* at 4:45–49.

Additionally, Figure 4 shows that cryptographic device 43 includes data stream interceptor 431 operatively coupled to a main controller 432.

Ex. 1001, 4:50–52. Main controller 432 communicates control signals to data generating controller 433, data storage controller 434, and cipher engine 436. *Id.* at 4:52–54. Main controller 432 receives input from data stream interceptor 431 and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, decrypted, or passed through unmodified. *Id.* at 4:55–58. The ’995 patent discloses that data stream interceptor 431 is adapted to distinguish between command/control and data signal transfers, and is configured to pass through certain command/control signals via bypass data path 44, and intercept other command/control signals which are transmitted to main controller 432. *Id.* at 4:58–65. Main controller 432 also “instructs data generating controller 433 and data storage controller 434 to perform specific data transfer protocols . . . of data generating device 41 and data storage device 42, respectively, according to the intercepted command/control signals.” *Id.* at 4:65–5:4.

As discussed previously, Figure 4 shows cipher engine 436. “Main controller 432 also transmits control signals to cipher engine 436 to notify the same of an incoming data stream.” Ex. 1001, 5:4–6. Cipher engine 436 is programmed to transparently encrypt/decrypt streaming data during data transfer between data generating device 41 and data storage device 42. *Id.* at 5:6–11.

C. Illustrative Claim

Of the challenged claims, claims 1, 5, 9, 13, 14, and 15 are independent. Claim 9 is illustrative of the subject matter of the ’995 patent, and is reproduced below:

9. A cryptographic device, comprising:

> at least one data stream interceptor that distinguishes between command/control and data signal transfers;
>
> a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;
>
> at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;
>
> at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and
>
> at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

Ex. 1001: 6:45–64.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner contends that the level of ordinary skill in the art is a bachelor's degree in electrical or computer engineering or computer science, and two years of experience in a relevant field of computer data storage, data transmission, and encryption "or . . . equivalent knowledge and experience." Pet. 13 (citing Ex. 1006 ¶¶ 15–17). Patent Owner disagrees and urges a different level of ordinary skill in the art as a bachelor's degree in electrical and/or computer engineering, plus either a master's degree in one of those fields or two years of industrial experience in the technical fields of Application-Specific Integrated Circuit (ASIC) design, hard drive data transfer protocols, and encryption standards, or equivalent knowledge and experience. PO Resp. 12–13. Patent Owner further argues that a "person of

ordinary skill in the art of the ’995 patent should have experience with hardware systems and related prior art, which persons with a pure software background and a computer science degree do not necessarily have.” *Id.* at 13.

To determine the level of ordinary skill in the art in this case, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, and the sophistication of the technology. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986). Also, we are guided by the level of ordinary skill in the art as reflected by the prior art of record. *Okajima v. Bourdeau*, 261 F.3d. 1350, 1355 (Fed. Cir. 2001).

We are persuaded by the parties’ contentions that the level of skill in the art would include a bachelor’s degree in electrical or computer engineering or computer science and either a master’s degree or two years of experience in a relevant field such as computer data storage, data transmission (e.g., data transfer protocols), and encryption. Pet. 13; PO Resp. 13. We, however, do not agree with Patent Owner that the relevant field of experience must include hardware encryption experience and excludes persons having a software background or a degree in computer science. PO Resp. 13; Ex. 2013 ¶ 42. Although the Specification of the ’995 patent and the challenged claims disclose a “cryptographic device,” we do not agree with Patent Owner that the use of “device” in this manner excludes software-based encryption. Indeed, the ’995 patent teaches that encryption can be performed by either conventional software-based applications or hardware devices available. Ex. 1001, 1:35–2:3. Additionally, Petitioner’s declarant, Dr. Darrell Long, testifies that

> [p]ersons of ordinary skill in the art at the time of the filing of the ’995 Application also understood that encryption was typically implemented using one of two methods: software-based encryption or hardware-based encryption. Software-based encryption typically relied on software in the host computer, executed by the host [central processing unit (CPU)], to run the necessary encryption algorithm. It was well-known at the time of the filing of the ’995 Application that software-based encryption was typically slower than hardware-based encryption, as it used the host computer’s CPU to perform the encryption. Hardware-based encryption, in contrast, was typically faster as it was performed by dedicated hardware, such as dedicated PCMCIA [Personal Computer Memory Card International Association] cards plugged into the host or external ASIC-based devices.

Ex. 1006 ¶ 32 (citing Ex. 1001, 1:38–40).

Moreover, the level of skill in the art as reflected in the prior art of record encompasses both software-based and hardware-based encryption. For example, Nolan does not restrict encryption methods to software applications or hardware devices and describes the use of key-based “[m]odern encryption algorithms.” Ex. 1002, 5:3–5.[5] Thus, when considering the entire evidence of record, we conclude that a person of ordinary skill in the art at the time of the ’995 patent would have had a bachelor’s degree in electrical or computer engineering or computer science and either a master’s degree or two years of experience in a relevant field such as computer data storage, data transmission (e.g., data transfer protocols), and encryption.

[5] All page numbers of Exhibit 1002 refer to the page numbers located at the bottom, right-hand portion.

B. Weight Given to Petitioner's Declarant, Dr. Long

Patent Owner asserts that Petitioner's declarant, Dr. Long, is not qualified to provide expert testimony in this proceeding because Dr. Long does not have sufficient experience with hardware. PO Resp. 12. Specifically, Patent Owner asserts that Dr. Long has experience in computer data transmissions, data storage, and data security at the systems level, but lacks hardware encryption experience. *Id.* at 13. Patent Owner further asserts that Dr. Long's testimony is entitled to little weight because he does not fully understand the SCSI-2 Specification and provides "erroneous information that confuses and oversimplifies critical aspects of the SCSI-2 Specification." *Id.* at 14; *see id.* at 16. Patent Owner further contends Dr. Long's business affiliation with Petitioner indicates Dr. Long's testimony is biased.

First, we do not agree with Patent Owner that Dr. Long is not qualified to provide expert testimony because he does not have hardware-based encryption experience. As discussed above, we determine that the level of skill in the art at the time of the filing of the '995 patent does not exclude persons having software-based instead of hardware-based encryption experience. Moreover, we note that generally, arguments that the scientific or technical experience and knowledge of Dr. Long do not match the alleged level of skill in the art are unpersuasive as there is no requirement of a perfect match between the expert's experience and the field of the art in question. *See SEB S.A. v. Montgomery Ward & Co., Inc.*, 594 F.3d 1360, 1373 (Fed. Cir. 2010).

Second, a declarant may be qualified as an expert if the declarant's scientific, technical, or other specialized knowledge will help the trier of fact

to understand the evidence or to determine a fact in issue. Fed. R. Evid. 702. Patent Owner has not filed a motion to exclude on the basis of competency of Petitioner's expert witness, Dr. Long, and, therefore, we do not undertake an analysis of whether Dr. Long is, indeed, qualified under the Federal Rules of Evidence. We do note, however, that Dr. Long has experience in the field of computer data transmissions, data storage, and data security, including experience with security and encryption for hard disk drives. Ex. 1006 ¶ 5; *see also* Ex. 1014 (Dr. Long's Curriculum Vitae).

Additionally, we are capable of discerning from the testimony and the evidence presented the expertise and any potential bias of a witness, and then attributing the appropriate weight to the witness's testimony. *See, e.g.*, *Ethicon, Inc. v. U.S. Surgical Corp.*, 135 F.3d 1456, 1465 (Fed. Cir. 1998) ("a witness's pecuniary interest in the outcome of a case goes to the probative weight of testimony, not its admissibility"). With these considerations in mind, we now turn to the construction of certain claim terms.

C. Claim Construction

In an *inter partes* review, "[a] claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b); *see also In re Cuozzo Speed Technologies, LLC*, No. 2014-1301, 2015 WL 4097949, at *7–*8 (Fed. Cir. July 8, 2015) ("We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA" and "the standard was properly adopted by PTO regulation."), *reh'g en banc denied*, 2015 WL 4100060 (Fed. Cir. July 8, 2015). There is a "heavy presumption" that a claim term carries its ordinary and customary meaning.

CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366 (Fed. Cir. 2002); *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

1. *data stream interceptor that distinguishes between command/control and data signal transfers (claims 1, 5, 9, and 13–15)*

For purposes of our Decision to Institute, we determined that the phrase "data stream interceptor that distinguishes between command/control and data signal transfers" should be construed as "one or more components adapted to intercept at least one data stream and distinguish the command or control signals *in the data stream* from the data signals" as proposed by the Petitioner. Dec. to Inst. 7–8 (citing Pet. 10; Ex. 1001, 4:32–35, 55–65).

In its Patent Owner Response, Patent Owner asserts that its construction for "data stream interceptor" as proposed in the Preliminary Response is based on the plain language of the claims and is consistent with the claim construction in the district court in *Enova v. WD*. PO Resp. 9–10 (citing Exs. 2001–2002). Specifically, Patent Owner proposes the construction of "one or more components adapted to intercept at least one data stream and distinguish between command/control signal transfers and data signal transfers." Prelim. Resp. 10–11 (citing Ex. 2001, 7). Patent Owner further asserts that the term "interceptor" requires "some level of examination of the data stream itself by, for example *extracting some of the data in the data stream*, which then allows the data stream interceptor to distinguish which parts of the data stream are command/control signal transfers" and data signal transfers. PO Resp. 19 (emphasis added). Patent Owner adds that the "interceptor" must do something more than allow the "passing through" of signals. *Id.*; Tr. 36:22–37:21, 38:23–39:19.

In the Reply, Petitioner responds that it has not argued that “intercepting” is synonymous with “passing through” via a bypass line. Reply 1; Tr. 9:5–10:3. Rather, Petitioner argues that it used the phrase “passing through” in the Petition to refer to receiving and acting on information. *Id.* Petitioner adds that “the broadest reasonable construction of intercept is simply are you . . . receiving it and doing something with it.” Tr. 8:6–8. According to Petitioner, this is the ordinary and customary meaning of “intercept,” which is consistent with the Specification’s disclosure that the “data stream interceptor intercepts commands and sends them to the main controller.” *Id.* at 8:11–20; *see* Reply 2. Petitioner further argues the Specification of the ’995 patent does not limit what “intercepting” covers or give the term a special meaning such as “‘examining’ or ‘extracting’ signals.” Reply 2; Tr. 7:21–8:8.

Based on the complete record before us, we agree with the parties that the broadest reasonable interpretation of the term “intercept” is the plain, ordinary, and customary meaning, which is *to receive and act upon*. The Specification does not expressly define “interceptor”; however, the plain, ordinary, and customary meaning of “intercept” is “to receive (a communication or signal directed elsewhere) usually secretly” and “to stop, seize, or interrupt in progress or course or before arrival.” MERRIAM WEBSTER’S COLLEGIATE DICTIONARY (Frederick C. Mish et al., 10th ed. 1997) (Ex. 3002). This definition is consistent with the Specification, which discloses “interceptor 431 is configured to pass through certain command/control signals via a bypass data path 44, and intercept other command/control signals which are transmitted to main controller 432.” Ex. 1001, 4:55–65.

We further note that, in discussing the prior art references, Patent Owner asserts that the "distinguishing function of the data stream interceptor cannot be independent from the intercepting and from the data stream itself," and the distinguishing of signals cannot occur before a data stream is present. PO Resp. 20–25; *see* Tr. 44:12–46:14. Essentially, Patent Owner asserts that the claim language requires a specific manner of distinguishing in a data stream. However, we do not agree that the term "distinguishes" requires any such limitation. The literal language of the claim does not limit how the data stream interceptor distinguishes the signals in the data stream. This is consistent with the Specification, which also does not limit how signals are distinguished. Ex. 1001, 4:58–65. Moreover, Patent Owner conceded that, for the purposes of this proceeding, it agrees with the Board's construction in the Decision to Institute. Tr. 46:15–25. Thus, we discern no sufficient reason to alter or depart from our claim construction of the phrase "data stream interceptor that distinguishes between command/control and data signal transfers" as "one or more components adapted to intercept at least one data stream and distinguish the command or control signals in the data stream from the data signals." We do, nonetheless, clarify that the plain, ordinary, and customary meaning of "intercept" applies and that distinguishing signals in the data stream can be performed in any manner.

2. "transparently" (claims 1, 5, 9, and 13–15)

In the Decision to Institute, we determined that the broadest reasonable interpretation of "transparently" is "functionally invisible" because this construction is consistent with the ordinary and customary meaning of "transparent" as would be understood by one with ordinary skill in the art in light of the '995 patent. Dec. to Inst. 9–11 (citing Ex. 1001,

3:34–36; Ex. 3001, 3).

Patent Owner argues that its proposed construction of "functionally, data transfers appear to be performed directly between the data generating device and the data storage device" (Prelim. Resp. 13–14) is directly supported by the Specification as describing transparent encryption. PO Resp. 10–11 (citing Ex. 1001, 3:62–4:2, 4:21–29). As we noted in the Decision to Institute, Patent Owner's proposal is more restrictive than the claim language, which does not recite explicitly that data transfers appear to be performed directly between the data generating device and data storage device. Moreover, Patent Owner's proposed construction ignores the Specification's disclosure that an "invisible" cryptographic device also functionally performs data transfers "directly between data generating device 13 and/or data storage device 11, respectively." Ex. 1001, 3:30–34. Although the Specification does not expressly define "transparently," it does describe the disclosed cryptographic device as an "invisible" data transfer bridge connecting data generating device 13 and data storage device 11. Ex. 1001, 3:34–36. This disclosure is consistent with the ordinary and customary meaning of "transparently," which is "[i]n computer use, of, pertaining to, or characteristic of a device, function, or part of a program that works so smoothly and easily that it is invisible to the user." Ex. 3001, 3. Accordingly, we maintain that the broadest reasonable interpretation of "transparently" is "functionally invisible."

3. "input" (claims 1, 5, 9, and 13–15)

In the Decision to Institute, we did not adopt Patent Owner's proposed construction of "input" and determined that the claim term does not require *input distinguishing between command/control and data signal transfers*,

but rather encompasses either command/control or data signals. Dec. to Inst. 11–12. In response, Patent Owner contends that our construction is inconsistent with the district court's construction in *Enova v. WD*. PO Resp. 11. Specifically, Patent Owner argues that the district court's construction provides a link between "input" and the determination of whether to encrypt/decrypt or pass through each signal. *Id.* (citing Ex. 1001, 4:55–61). Patent Owner asserts that the district court's construction requires "input" resulting from the distinguishing to be sent to and used in some way by the main controller in determining. *Id.* at 11–12 (citing Ex. 2002, 2).

Although the district court's claim construction in *Enova v. WD* is informative and provides some guidance on the interpretation of the term "input," we are not bound by the district court's findings. Rather, we apply the broadest reasonable interpretation standard in this proceeding, under which we determined in the Decision to Institute that the term "input" does not require a specific type of input. This interpretation is consistent with the Specification, which teaches "[m]ain controller 432 receives input from data stream interceptor 431 and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, decrypted or passed through unmodified." Ex. 1001, 4:55–58. The Specification does not limit the described input to a type of information such as that which distinguishes between signals. Based on the entire record before us, we discern no reason to alter our claim construction for "input" for this Final Written Decision.

4. *"A cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer" (claim 13);*

   A cryptographic device integrated within a data storage device for use during data transfer with a data generating device (claim 14); and

   A cryptographic device integrated within a data generating device for use during data transfer with a data storage device (claim 15).

For the Decision to Institute, we concluded that the limitations recited in the body of claims 13, 14, and 15 essentially are identical except for the language of the preambles, which indicate the location of the cryptographic device and provide the only difference in claim scope between claims 13, 14, and 15. Dec. to Inst. 13. We further determined that the preambles are essential to understand the scope of claims 13, 14, and 15, and operate as claim limitations. *Id.* In Patent Owner's Response, Patent Owner reserved the right to challenge our construction, but did not explain how the preambles should be construed. PO Resp. 11. Accordingly, based on the complete record before us, we maintain that the preambles of claims 13, 14, and 15 are limiting.

D. Claims 1–13 – Obviousness over Nolan (Ex. 1002) and SCSI-2 (Ex. 1003)

Petitioner argues claims 1–13 are unpatentable under 35 U.S.C. § 103(a) over Nolan and SCSI-2. Pet. 15–40. Patent Owner contests Petitioner's position. PO Resp.17–46. As explained below, we have considered the arguments and evidence presented by both parties, and we determine Petitioner has shown by a preponderance of the evidence that claims 1–13 are unpatentable over Nolan and SCSI-2.

1. Summary of Nolan (Ex. 1002)

Nolan describes an apparatus for encrypting computer data before storage. Ex. 1002, 5:1–2. Figure 1 (reproduced below) shows a block diagram of an apparatus for encryption that is designed for use with tape drives that use a Small Computer System Interface (SCSI). *Id.* at 8:8–10, 13–15.

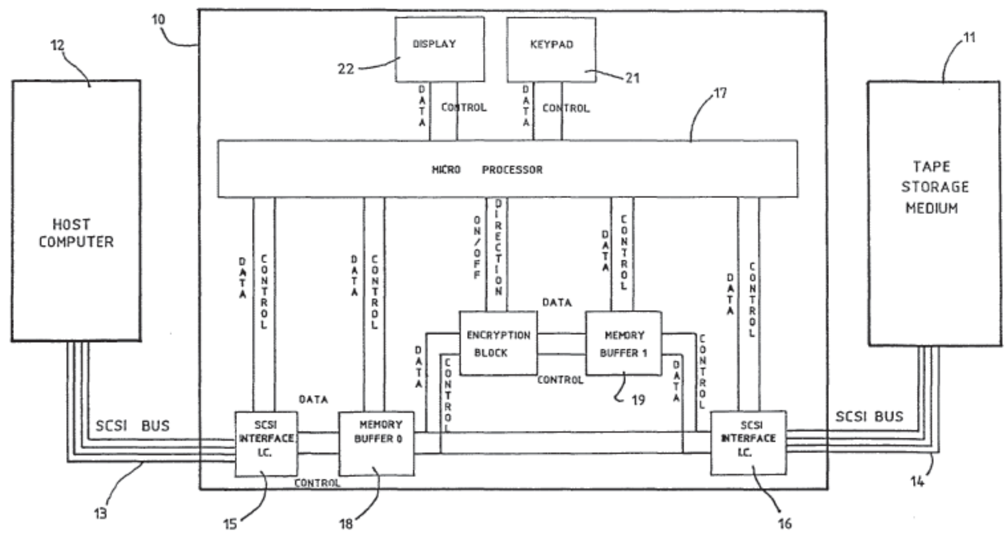


FIG 1

Figure 1 shows encryption/decryption apparatus 10 connected to host computer 12 and tape storage medium 11 via a SCSI BUS. Encryption and decryption apparatus 10 includes host computer interface 15 and tape drive interface 16 on respective sides. Ex. 1002, 8:25–26.

Encryption/decryption apparatus 10 includes an encryption block and microprocessor 17. Under the control of the microprocessor 17, host computer interface 15, tape drive interface 16, and the encryption block transfer data to or from host memory buffer 18 or target memory buffer 19. *Id.* at 8:27–9:8. Whether a particular memory block responds to a request signal is controlled by microprocessor 17. Microprocessor 17 can switch on

and off the flow of data into and out of a particular memory buffer from a particular source or destination. *Id.* at 9:13–18. Microprocessor 17 also sets the encryption block to encrypt or decrypt, and transfers data through the encryption block from a memory buffer. *Id.* at 9:25–6:2.

Additionally, Nolan's Figure 2 shows a flow diagram of the main program steps performed by microprocessor 17. Ex. 1002, 10:12–13. After initiation 30 and 31, microprocessor 17 reads the common encryption key stored on the tape and stores it in encryption/decryption apparatus 10. *Id*. at 10:14–16. "[M]icroprocessor 17 waits for a command to be sent from the host computer, step 32" ("Wait for Input SCSI Command"). *Id.* at 10:17–18. If the command involves tape movement, "the anticipated amount of movement is calculated and stored, step 35." *Id.* at 10:21–23. "The microprocessor then ascertains whether any transfer of encrypted data is required, steps 36 and 37." *Id.* at 10:23–25. "If not, the command is executed, step 38." *Id.* "If it does involve the transfer of encrypted data then the stored encryption key is modified by the current tape position, step 39." *Id.* at 10:26–29.

2. Summary of SCSI-2 (Ex. 1003)

SCSI-2 describes SCSI as a local input/output (I/O) bus that can be operated over a wide range of data rates. Ex. 1003, 35.[6] "When two SCSI devices communicate on the SCSI bus, one acts as an initiator and the other acts as a target. The initiator originates an operation and the target performs the operation." *Id.* at 59.

[6] All page numbers for SCSI-2 refer to the page number located in the bottom, right-hand corner.

SCSI-2 discloses that the SCSI architecture includes eight distinct phases: (a) BUS Free phase, (b) ARBITRATION phase, (c) SELECTION phase, (d) RESELECTION phase, (e) COMMAND phase, (f) DATA phase, (g) STATUS phase, and (h) MESSAGE phase. Ex. 1003, 68. SCSI-2 adds that the SCSI bus "can never be in more than one phase at any given time." *Id.* SCSI-2 also refers to the COMMAND, DATA, STATUS, and MESSAGE phases, collectively, as information transfer phases because "they are all used to transfer data or control information via the DATA BUS." Ex. 1003, 71.

SCSI-2 also discloses that SCSI bus signals include an I/O signal, a C/D (CONTROL/DATA) signal, and a MSG (MESSAGE) signal. Ex. 1003, 61. The C/D signal is "driven by a target that indicates whether CONTROL or DATA information is on the DATA BUS. True indicates CONTROL." *Id.* SCSI-2 further discloses "[e]ach signal driven by an SCSI device shall have" a lower voltage of 0 to 0.5 volts for signal assertion and a higher level voltage of 2.5 to 5.25 volts for signal negation. *Id.* at 54. Additionally, the C/D, I/O and MSG signals are used to distinguish between the different information transfer phases. *Id.* at 71. The "target drives these three signals and therefore controls all changes from one phase to another." *Id.* Table 8 (reproduced below) shows the use of C/D, I/O, and MSG signals. *Id.* at 72.

Table 8 - Information transfer phases

Signal			Phase name	Direction of transfer	Comment
MSG	C/D	I/O			
0	0	0	DATA OUT	Initiator to target \	Data phase
0	0	1	DATA IN	Initiator from target /	
0	1	0	COMMAND	Initiator to target	
0	1	1	STATUS	Initiator from target	
1	0	0	*		
1	0	1	*		
1	1	0	MESSAGE OUT	Initiator to target \	Message phase
1	1	1	MESSAGE IN	Initiator from target /	
Key: 0 = False, 1 = True, * = Reserved for future standardization					

As shown in Table 8, during the DATA phase, the C/D signal indicates False. *Id.* During the COMMAND phase, the C/D signal indicates True. *Id.*

3. Analysis

Below we discuss independent claim 9, which is illustrative of challenged claims 1–8 and 10–13. Claim 9 recites a cryptographic device comprising “at least one data stream interceptor that distinguishes between command/control and data signal transfers.” Ex. 1001, 6:46–47.

Petitioner asserts that Nolan’s disclosure of SCSI Interface 15 implemented using the details of SCSI-2 teaches this limitation. Pet. 19. More particularly, Petitioner points to Figure 1 of Nolan to show all data streams originating from host computer 12 travel over SCSI bus 13 and are intercepted by SCSI Interface 15 when entering encryption/decryption apparatus 10. *Id.* Petitioner further argues Nolan’s SCSI Interface 15 distinguishes between command/control signals and data signals by using the C/D signal disclosed in SCSI-2. *Id.* at 20.

Additionally, Petitioner asserts a person of ordinary skill in the art would have been motivated to combine Nolan’s cryptographic device with SCSI-2, because Nolan explicitly teaches the use of SCSI to transfer data

between the host computer and the storage medium. Pet. 17 (citing Ex. 1002, 4:13–15). Petitioner's declarant, Dr. Long, also testifies that:

> The embodiment in Figure 1 of Nolan is implemented using multiple "SCSI bus[es]" and "SCSI Interface[s]" 15 and 16. (*Id.* at Figure 2.) The specification repeats that Nolan can be implemented using "SCSI commands" (*see* Figure 2) and other features detailed in the "SCSI-1 and SCSI-2" protocols (*id.* at 8:25). In my opinion, these teachings would have directed one of ordinary skill to look to the SCSI-2 Specification for specific details of how the SCSI protocol operates in Nolan.

Ex. 1006 ¶ 58.

Patent Owner argues that the combination of Nolan and SCSI-2 does not teach a data stream interceptor that intercepts data streams and performs the claimed distinguishing function. PO Resp. 17. Patent Owner first asserts that Petitioner argues SCSI Interface 15 intercepts data streams because data from host computer 12 travels over SCSI bus 13 and "pass through" SCSI Interface 15. *Id.* at 18. Patent Owner contends that "passing through" and "intercepting" are different functions in the context of the '995 patent (*id.* at 19 (citing Ex. 2013 ¶ 83)), and intercepting the data stream as claimed requires "examination of the data stream itself by, for example, extracting some of the data in the data stream, which then allows the data stream interceptor to distinguish which parts of the data stream are command/control signal transfers and which parts of the data stream are data signal transfers." *Id.* at 19 (citing Ex. 2013 ¶ 84); Tr. 36:22–37:9.

In its Reply, Petitioner responds that it used the phrase "passing through" in the Petition to describe that "all information [in Nolan] passes through in the sense that the information arrives at SCSI interface, it's interpreted, reviewed, and acted on." Reply 1; *see* Tr. 9:11–16. As an

example, Petitioner asserts that Nolan's SCSI Interface 15 does not have a bypass path and, therefore, intercepts all commands and sends them to the microprocessor. Reply 2; *see* Tr. 8:20–22. During oral argument, Petitioner clarifies that the '995 patent teaches an "almost identical" manner of interception in that the data stream interceptor *intercepts* commands and sends them to the main controller. Tr. 8:17–20.

First, we do not agree with Patent Owner that the ordinary and customary meaning of "intercept" requires examination of a data stream and extraction of data in the data stream. *See supra*, Section II.C.1.,Claim Construction. As discussed previously, we find that the ordinary and customary meaning of "intercept," is "to receive and act upon." Consistent with this interpretation, the Specification of the '995 patent describes data stream interceptor 431 as intercepting command/control signals, which are transmitted to main controller 432. Ex. 1001, 4:61–64. Thus, the scope of the term "intercept," as described in the '995 patent, encompasses *receiving* command/control signals and *transmitting* those signals elsewhere such as main controller 432. *See id.*

Second, turning to the disclosure in Nolan relied upon by Petitioner, SCSI Interface 15 performs interception in nearly the same manner as described by the '995 patent, namely, by receiving information from host computer 12 through SCSI bus 13 and transmitting data to host memory buffer 18 and commands to microprocessor 17. Ex. 1002, Fig. 1, 8:27–9:1. Moreover, according to Patent Owner and Patent Owner's declarant, Dr. Thomas Conte, "Nolan discloses that commands are sent to the microprocessor 17 and that data is sent to host memory buffer 18." Ex. 2013 ¶ 95 (citing Ex. 1002, 10:14–18, 5:9–19); PO Resp. 33. Thus, based on the

complete record, we agree with Petitioner that Nolan discloses a "data stream interceptor" that receives information and then transmits commands to a microprocessor and transmits data to a memory buffer.

Alternatively, Petitioner asserts that one of ordinary skill in the art would have understood that SCSI Interface 15 is adapted to route signals from entering data streams to internal registers for temporary storage and then to different locations within apparatus 10. Reply 1–2 (citing Ex. 1006 ¶¶ 76–78); Tr. 11:14–12:9. Petitioner relies on the testimony of Dr. Long and Exhibits 1017 and 1019 to show that a person of ordinary skill in the art would have possessed this background knowledge at or around the time the application leading to the '995 patent was filed. Reply 1–2 (citing Ex. 1006 ¶¶ 76–77). Patent Owner contends that Nolan does not provide this disclosure. PO Resp. 33–34. Despite Patent Owner's contention to the contrary, we credit the testimony of Dr. Long and the disclosures in Exhibits 1017 and 1019 and we find that knowledge of temporary registers may be imputed to a hypothetical person of ordinary skill for purposes of an obviousness analysis. *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013) (non-applied art or evidence may be considered as background information known to a person of ordinary skill in the art). Accordingly, based on Petitioner's alternative reasoning, we also agree that Nolan discloses a "data stream interceptor."

Next, Patent Owner argues that the combination of Nolan and SCSI-2 does not teach the distinguishing function of the "data stream interceptor." PO Resp. 19–34. Patent Owner argues that the selection of "Information Transfer Phases," as described in SCSI-2, by Nolan's SCSI Interface 15 does not distinguish between command/control and data signal transfers because

SCSI Interface 15 presumes the incoming signals will correspond to the information transfer phase that has been selected previously. PO Resp. 20–22 ("SCSI Interface 15 knows, based on the information transfer phase it has set, what kind of signal is incoming and can act accordingly. It need not 'distinguish' between signal types when that signal has already been divided into neat buckets for it."); Tr. 40:20–23 ("We think that SCSI interface 15 is commanding or setting the data transfer phase, and that it does not do any distinguishing through these voltages.").

Patent Owner further argues that, during a SCSI data transmission, the selection of an information transfer phase, such as COMMAND or DATA (represented by a C/D signal) on a control wire, is subsequently followed by the transmission of a data stream on the DATA BUS. PO Resp. 22–24. Specifically, Patent Owner argues that SCSI-2 teaches the transmission of a data stream over the DATA BUS does not occur until after the C/D signal is set (information transfer phase selected) and a REQ/ACK handshake protocol is satisfied. *Id.* at 23–24. Patent Owner asserts that the C/D signal on the control wire is not part of the data stream that is transferred over the DATA BUS cables and SCSI Interface 15 cannot distinguish command or control signals in the data stream from the data signals because there is no data stream at the time the C/D signal is driven by SCSI Interface 15. *Id.* at 23–24.

In response, Petitioner argues that the claims do not restrict how or when distinguishing may occur and that SCSI Interface 15 distinguishes the type of incoming signal based on the information transfer phrase selected. Reply 4–6 ("The '995 Patent places no restrictions on which signals may be used to perform the distinguishing function, and provides no particular

method for distinguishing.”). Petitioner adds that, “even if a timing limitation were justified, the SCSI-2 Specification teaches that the C/D signals are maintained throughout each phase so that Nolan’s SCSI Interface 15 continues to distinguish command/control signals from data signals as those signals travel on the DATA BUS.” *Id.* at 5 (citing Ex. 1003, 71 n.25, 431, Fig. A1).

We agree with Petitioner and find that the ordinary and customary meaning of “distinguishes,” as recited in claim 9, does not require a specific manner of distinguishing. *See supra* Section II.C.1., Claim Construction. For example, the claim language does not require the recited data stream interceptor to distinguish command/control signals and data signals by using signals in the data stream. Further, the claim language does not impose a timing requirement as to when the distinguishing must or cannot occur.

Additionally, Patent Owner asserts that SCSI-2 does not distinguish between command/control signals and data signals because the SCSI-2 does not distinguish user data from non-user data. PO Resp. 26–29. Patent Owner argues that the use of the term “DATA” in SCSI-2 is not the same as the “data signals” recited in the claims of the ’995 patent because both user data and non-user data are transferred during the “DATA” phase. PO Resp. 26–27 (citing Ex. 2013 ¶¶ 73, 93). Patent Owner’s declarant, Dr. Conte, further testifies that SCSI-2 discloses

> certain commands, such as INQUIRY, result in “data” sent across the bus during a DATA phase that is not in fact user data but other data, which Dr. Long defines as a control signal (responsive to the inquiry from another device). In the case of INQUIRY, it includes information about the SCSI target’s capabilities as well as vendor information. *See supra* ¶ 73. This is clearly not user data or data signals as claimed. Second, there are commands in the SCSI-2 protocol that include

> parameters that are sent from the initiator to the target during the DATA OUT phase, such as the COPY command. A person of ordinary skill in the art would consider these command parameters as "command signals," rather than "data signals," within the meaning of the '995 patent.

Ex. 2013 ¶ 93. Patent Owner adds that Nolan also does not distinguish between user data and non-user because it discloses an embodiment in which all data sent through the data bus would be encrypted, including commands. PO Resp. 29 (citing Ex. 1002, 12:18–20). Patent Owner further argues that Petitioner's declarant, Dr. Long, has not explained sufficiently how a skilled artisan would distinguish between user data and non-user data based on Nolan and SCSI-2. *Id.* at 28.

In response, Petitioner asserts that the '995 Patent "requires only that the interceptor be adapted to distinguish command or control signals from data signals—*i.e.*, user data—in at least one data stream, which SCSI Interface 15 does in the data streams for the READ(6) and WRITE(6) operations using the C/D line, as discussed above." Reply 6. Petitioner further contends that Patent Owner's citation to an alternative embodiment in Nolan does not diminish Nolan's disclosure of other embodiments where SCSI Interface 15 implemented with SCSI-2 would perform the claimed distinguishing function. *Id.* at 7.

First, we agree with Petitioner that Nolan's description of one embodiment with complete encryption/decryption of data does not discount Nolan's concurrent disclosure of other embodiments in which encryption/decryption is optional. *See* Ex. 1002, 5:20–28. Second, we agree with Petitioner that the claim language "data stream interceptor that distinguishes between command/control and data signal transfers" does not

require the interceptor to distinguish between user data and non-user date. We also agree with Petitioner that SCSI-2's READ(6) and WRITE(6) operations describe at least one instance where information transfer phases distinguish between command/control signals and data signals. Pet. 19 (citing Ex. 1006 ¶¶ 99–107); Reply 6 n.2, 8 n.3 (citing Ex. 1006 ¶ 105; Ex. 1029, 61:10–17; 62:6–23; 67:6–11; 68:1–10.

A better understanding of SCSI-2's READ(6) and WRITE (6) operations can be derived by looking at, for example, Table 22 of SCSI-2 reproduced below.

Table 122 - READ(6) command

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation code (08h)							
1	Logical unit number			(MSB)				
2	Logical block address							
3								(LSB)
4	Transfer length							
5	Control							

Table 2 shows the command block of READ(6). Ex. 1003, 197. During cross-examination, Patent Owner's declarant, Dr. Conte, testified that the READ(6) command block, shown in Table 22, is an example of a SCSI-2 command used to transfer user data from a storage device to a host computer. Ex. 1029, 61:10–17. Dr. Conte further testified that "there's no additional parameters to the READ(6) command beyond what's in the 6 bytes in the command block." and that the READ(6) command is sent during the command phase of a data transfer operation. *Id.* at 62:6–63:7. Dr. Conte also agreed that user data would be sent in a data phrase of the data transfer operation. *Id.* at 63:8–15. Additionally, Dr. Conte acknowledged that the fourth paragraph on page 102 of SCSI-2 describes: (1) an example of a single SCSI-2 command, such as a READ command; and (2) transfer of the command descriptor block during the COMMAND phase and transfer of

data during the DATA IN phase. *Id.* at 65:7–66:17. Thus, we agree with Petitioner that operation of the READ(6) command involves the selection of COMMAND phase to transmit the READ command and the selection of the DATA IN phase to transmit data.

At the oral hearing, Patent Owner argued that the Petition did not contain the READ(6) and WRITE(6) arguments because Petitioner relied generally on the C/D wire "theory" without limiting that theory to read or write commands. Tr. 47:12–48:12. However, when discussing how Nolan's SCSI Interface 15 is capable of distinguishing between command/control signals and data signals on page 19 of the Petition, Petitioner refers to paragraphs 99–107 of Dr. Long's declaration. The relevant portion of paragraph 105 states:

> when data is being sent from the host computer, encrypted, and written on the tape drive, SCSI Interface 15 distinguishes the "write" command sent from the host computer from data sent from the host computer. Likewise, when data is being read from the tape drive, decrypted, and sent to the host computer, SCSI Interface 15 distinguishes the "read" command sent from the host computer from data.

Ex. 1006 ¶ 105.

Moreover, Patent Owner was given an opportunity to address the READ(6) and WRITE(6) arguments at the oral hearing. Tr. 47:12–51:23. At the oral hearing, Patent Owner argued that Petitioner's theory that SCSI-2's C/D wire distinguishes between command/control and signals and data signals is not supported by the description of the READ(6) and WRITE(6) commands because SCSI-2 discloses other commands, i.e., INQUIRY and COPY commands, where command signals are transmitted during the DATA phase. Tr. 47:3–50:9. We do not agree with Patent Owner's

arguments because, as discussed above, Petitioner has explained sufficiently that SCSI-2 teaches the C/D wire distinguishes command/control and data signal for at least one data stream, which is shown in SCSI-2's READ(6) and WRITE(6) operations.

In the Patent Owner Response, Patent Owner further argues that SCSI-2's INQUIRY and COPY commands demonstrate that the status of the C/D wire cannot distinguish between data signals and control/command signals sent during a DATA phase. PO Resp. 30–33. Patent Owner additionally argues that Petitioner's reliance on temporary registers for the distinguishing functionality is not supported by the references. *Id.* at 33–34. We do not agree with Patent Owner's arguments. Instead, upon considering the complete record before us, we agree with Petitioner that the operation of SCSI-2's READ(6) and WRITE(6) commands teaches sufficiently how the signal of the C/D wire distinguishes between data signals and control/command signals.

Claim 9 further recites "a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor." Ex. 1001, 6:48–52.

Petitioner argues Nolan's disclosure of microprocessor 17 receiving input from SCSI Interface 15 meets this limitation. Pet. 23–24. Petitioner explains that Nolan's Figure 1 shows that microprocessor 17 receives input from SCSI Interface 15. *Id.* at 24. Petitioner's declarant, Dr. Long, adds "SCSI bus 13 connects host computer 12 to SCSI Interface 15 and transfers data through SCSI bus 13 using the SCSI protocol." Ex. 1006 ¶ 124 (citing Ex. 1002, Fig. 1, 4:17–26). Petitioner further argues Figure 2 of Nolan

shows a flowchart with a "WAIT FOR INPUT SCSI COMMAND," shown as step 32. Pet. 24. Petitioner explains that microprocessor 17 receives the input SCSI command from SCSI Interface 15, and "whenever input received from SCSI Interface 15 indicates a data transfer (step 36), microprocessor 17 makes a determination as to whether encryption or decryption is required (step 37)." *Id.* at 24–25.

Patent Owner argues Nolan's microprocessor 17 does not determine whether to encrypt or decrypt data based on a SCSI command received from SCSI Interface 15. PO Resp. 35–36 (citing Ex. 2013 ¶ 101) ("That the microcontroller 17 may make a determination of whether to encrypt or decrypt 'whenever input [is] received' does not show that any such determination is based on that input."); Tr. 59:14–18. Referring to Figure 2 of Nolan, Patent Owner asserts Petitioner does not provide a link between the alleged "input," a host SCSI command, and the decision to encrypt because tape movement is the only determination Nolan discloses as based on the command, and whenever input received from SCSI Interface 15 indicates a data transfer (Fig. 2, step 36), microprocessor 17 makes a determination as to whether encryption or decryption is required (Fig. 2, step 37). PO Resp. 36–37 (citing Ex. 1002, Fig. 2, 10:18–25). Additionally, Patent Owner argues that Nolan does not describe how step 37, "ENC/DEC REQUIRED?" (Ex. 1002, Fig. 2), is performed, but asserts that this step is likely based on checking a configuration setting provided by a user (e.g., through keypad 21). PO Resp. 39–42. Patent Owner also refers to examples disclosed in Detrick and Hamlin, describing encryption based on user configured settings, as showing that one of ordinary skill in the art would not have understood Nolan as teaching encryption based on the SCSI input

command. *Id.* at 41–42. Patent Owner further asserts that the INQUIRY command disclosed in SCSI-2 demonstrates a command that may require tape movement in Nolan without requiring encryption/decryption of the control information. *Id.* at 37–38 (citing Ex. 2013 ¶ 102); Tr. 57:17–58:10.

In response, Petitioner argues "the only input in Figure 2 [of Nolan] for the tape movement (step 33), data transfer (step 36), and encryption/decryption of the transferred data (step 37) is the SCSI command, indicating that each decision is based on the SCSI command." Reply 11 (citing Ex. 1002, Fig. 2).

We agree with Petitioner that Nolan sufficiently teaches microprocessor 17 determines "whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor" because the claim language does not require that the recited determination is based *directly* or *wholly* on the received input (i.e., SCSI command at step 32). Figure 2 of Nolan is reproduced below.

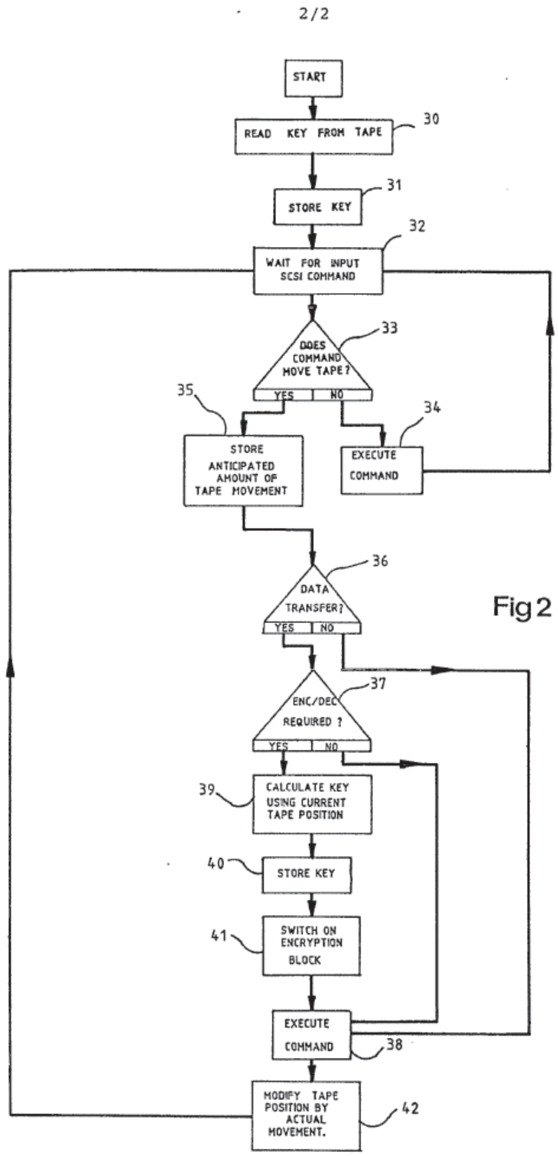


Fig 2

Figure 2 shows a flow diagram of the main program steps *controlling* the microprocessor 17. Ex. 1002, 6:12–13 (emphasis added). Figure 2 indicates, at step 32, microprocessor 17 waits for a SCSI command to be sent from the host computer. *Id.* at 6:17–18. If the SCSI command requires tape movement (step 33), microprocessor 17 continues to step 35 to determine the amount of tape movement, and then to steps 36 and 37 to "ascertain[] whether any transfer of encrypted data is required." *Id.* at 6:21–

25. Accordingly, microprocessor 17 may perform step 37, "ENC/DEC REQUIRED," only after microprocessor 17 receives the SCSI command at step 32, and determines the SCSI command involves tape movement at step 33 and data transfer at step 36. Although encryption or decryption determination at step 37 does not occur directly after step 32, receipt of the SCSI command prompts microprocessor 17 to determine whether to perform steps 33 and 35–37.

Furthermore, we do not agree with Patent Owner's arguments regarding SCSI-2's INQUIRY command, Nolan's alternative embodiment (e.g., keypad 21), or Detrick and Hamlin's teachings. As Patent Owner acknowledges, these arguments are based on "speculation," which we do not find detracts from or otherwise undermines Nolan's description of the embodiment shown in Figure 2. *See* Tr. 61:6–8.

Patent Owner further argues that based on the claim construction adopted by the district court in *Enova v. WD*, Nolan does not teach that the SCSI command is "input" that distinguishes between command/control and data signal transfers. PO Resp. 42–43. We have not adopted Patent Owner's construction for "input" and, therefore, do not agree that Nolan must teach a microprocessor receives input resulting from the distinguishing function performed by the data stream interceptor.

Claim 9 also recites

> at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

> at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller[.]

Ex. 1006, 6:53–60.

Petitioner argues that SCSI Interface 15 and 16 meet these limitations, because Nolan teaches that host computer interface 15 (also called SCSI Interface 15) "can, under the control of the microprocessor 17, transfer data directly to or from a host memory buffer 18," and SCSI Interface 16 transfers data between the tape storage medium and host memory buffer or target memory buffer under the control of microprocessor 17. Pet. 26 (citing Ex. 1002, 8:27–9:1). More specifically, Petitioner argues that Figure 1 of Nolan teaches that data transfers from memory buffers 18 and 19 by SCSI Interfaces 15 and 16 continue to the host computer and target. Reply 12–13. Petitioner further asserts that SCSI Interface 15 performs a data transfer protocol with the data generating device (host computer 12) on command from the main controller (microprocessor 17). Pet. 26 (citing Ex. 1002, Fig. 1, 4:17–26; Ex. 1006 ¶ 124). Petitioner also explains that "SCSI Interface 16 in Nolan (also called target tape drive interface 16), when implemented using the SCSI-2 Specification, performs a data transfer protocol with the data storage device (tape storage medium 11) on command from the main controller (microprocessor 17)." Pet. 27 (citing Ex. 1006 ¶ 128).

Patent Owner argues that Nolan does not teach SCSI Interface 15 is a data generating controller that performs a data transfer protocol with a data generating device because Nolan only describes moving data to internal memory buffers. PO Resp. 44 (citing Ex. 2012, 143:3–25; Ex. 2013 ¶ 108). For similar reasons, Patent Owner contends Nolan does not teach SCSI

Interface 16 is a data storage controller that performs a data transfer protocol with a data storage device. PO Resp. 45–46.

We agree with Petitioner's position. During cross-examination, Patent Owner's declarant, Dr. Conte, confirmed that SCSI Interfaces 15 and 16 communicate with the host computer and tape drive. Ex. 1029, 77:7–82:10; *see* Ex. 2013 ¶ 54. Moreover, we agree with Petitioner that Nolan's Figure 1, and accompanying description, discloses the use of the SCSI protocol with SCSI Interface 15 and 16 to communicate with memory buffers and the host computer 12 and tape storage medium 11, respectively. For example, Nolan teaches that host computer 12 is connected by SCSI cable 13 to encryption/decryption apparatus 10. Ex. 1002, 4:17–21. Nolan further teaches that SCSI Interface 15, under the control of microprocessor 17, can transfer data into or out of memory buffer 18. *Id.* at 4:25–5:1. As shown in Figure 1, data from host computer 12 can be transferred to memory buffer 18 via SCSI bus 13 and SCSI Interface 15. *Id.* at Fig. 1. Similar operations are disclosed for SCSI Interface 15, memory buffer 19, and tape storage medium 11.

Claim 9 also recites "at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller." Ex. 1001, 6:61–64. Petitioner argues "Nolan discloses a cipher engine—encryption block 20—situated within Nolan's cryptographic device ('apparatus 10') between the data generating device (host computer 12) and the data storage device (tape storage medium 11)." Pet. 29. Petitioner's declarant, Dr. Long, testifies that encryption block 20 performs data transfers transparently, because "[l]ike the cipher

engine in the ’995 Patent, Nolan’s encryption block 20 has its own dedicated microprocessor 17 as part of the encryption/decryption apparatus 10,” and “Nolan’s cryptographic device also uses the SCSI bus lines 13 and 14 that normally would have connected the host computer 12 directly to tape storage medium 11 without alteration.” *Id.* at 30 (quoting Ex. 1006 ¶ 133). Patent Owner does not address separately the cipher engine limitation in its Patent Owner Response. Applying our claim construction for the term “transparently,” we are satisfied that the disclosure in Nolan meets the cipher engine limitation.

Upon review of Petitioner’s evidence and analysis, and taking into account Patent Owner’s secondary consideration arguments discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claim 9 is unpatentable under 35 U.S.C. § 103 over Nolan and SCSI-2. Further, Petitioner provides detailed explanations of how each limitation of claims 2–13 is taught or suggested by the combination of Nolan and SCSI-2. Pet. 31–40. Patent Owner does not address separately these claims in its Patent Owner Response. *See generally* PO Resp. 17–46. We, therefore, adopt Petitioner’s explanations and supporting evidence as our own. Accordingly, we conclude after considering the complete record (including Patent Owner’s secondary consideration arguments) that Petitioner has established by a preponderance of the evidence that claims 2–13 would have been obvious over Nolan and SCSI-2.

E. Claim 14 – Obviousness over Nolan, SCSI-2, and Hamlin (Ex. 1004)

Petitioner argues claim 14 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Hamlin. Pet. 40–44. Specifically, Petitioner contends claims 13 and 14 contain the same limitations, except

that claim 14's preamble recites "[a] cryptographic device *integrated within a data storage device for use during data transfer with a data generating device*." *Id.* at 40 (emphasis added). As discussed above, we treat the preamble of claim 14 as limiting. *See supra* Section II.C.1.,Claim Construction. Patent Owner contests Petitioner's position. PO Resp. 47–48. As explained below, we have considered the arguments and evidence presented by both parties, and we determine Petitioner has shown by a preponderance of the evidence that claim 14 is unpatentable over Nolan, SCSI-2, and Hamlin.

1. Summary of Hamlin (Ex. 1004)

Hamlin is directed to the "need for a disk drive comprising a tamper resistant cryptosystem which is protected from an attacker employing chosen plaintext attacks." Ex. 1004, 2:3–5. Hamlin discloses "[a] disk drive comprising a disk for storing encrypted data." Ex. 1004, Abstract. Hamlin teaches second circuit 100, including encryption circuitry 110, that is housed within the disk drive. *Id.* at 2:66–3:3, Fig. 1.

2. Analysis

Petitioner argues Hamlin discloses encryption circuitry 110 connected to interface 104, which is "connected to receive user data from a host computer." Pet. 44 (citing Ex. 1004, Fig. 2, 4:18–22). Petitioner further asserts encryption circuit 110 is housed within disk drive, which is a data storage device. *Id.* at 43. Petitioner asserts that a person of ordinary skill in the art would have recognized the physical security of Nolan's cryptographic device (implemented using the SCSI-2 Specification), and particularly access to Nolan's SCSI bus, could be enhanced by housing Nolan's cryptographic device within a storage device, as taught by Hamlin. *Id.* at 44.

Patent Owner argues that Nolan and SCSI-2 does not disclose the recited data stream interceptor or main controller, and Hamlin does not supply the missing teaching. PO Resp. 47. For the same reasons discussed above with respect to claim 9, we agree with the Petitioner that the teachings in Nolan and SCSI-2 satisfy the data stream interceptor and main controller limitations recited in claim 14.

Patent Owner further contends that Nolan teaches the use of a keypad and display to configure apparatus 10 for encryption, and a person of ordinary skill in the art would not have combined a keyboard and display with Hamlin's disk drive (e.g., Figure 3 of Hamlin) because this would require incorporating a keypad and display inside Hamlin's circuit-based system. PO Resp. 47–48. Patent Owner also argues that Hamlin teaches away from using a keypad to enter a cryptographic key because this introduces potential vulnerabilities into Hamlin's system. *Id.* at 48.

Claim 14, however, does not require a keyboard or display, and Petitioner has not proposed the use of a keyboard or display with Hamlin's system. Petitioner explains that Hamlin teaches housing encryption circuitry within a disk drive improves system security, and that, based on this teaching, one of ordinary skill in the art would have recognized the security benefits of locating Nolan's cryptography device within a storage device. Pet. 44 (citing Ex. 1006 ¶ 177–178). Moreover, "[i]t is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements," but instead turns on "whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole." *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012).

Accordingly, upon review of Petitioner's evidence and analysis, and taking into account Patent Owner's secondary consideration arguments discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claim 14 is unpatentable under 35 U.S.C. § 103 over Nolan, SCSI-2, and Hamlin.

F. Claim 15 – Obviousness over Nolan, SCSI-2, and Detrick (Ex. 1005)

Petitioner argues claim 15 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Detrick. Pet. 44–49. Specifically, Petitioner contends claims 13 and 15 contain the same limitations, except that claim 15's preamble recites "a cryptographic device *integrated within a data generating device for use during data transfer with a data storage device*." *Id.* at 45 (emphasis added). As discussed above, we treat the preamble of claim 15 as limiting. *See supra* Section II.C.1.,Claim Construction. Patent Owner contests Petitioner's position. PO Resp. 48–50. As explained below, we have considered the arguments and evidence presented by both parties, and we determine Petitioner has shown by a preponderance of the evidence that claim 15 is unpatentable over Nolan, SCSI-2, and Detrick.

1. Summary of Detrick (Ex. 1005)

Detrick is directed to "implementing encryption and decryption of data stored from a computing system to a storage medium." Ex. 1005, 1:9–10. Figure 1 (reproduced below) shows an "embodiment of a computing system implementing encryption/decryption capabilities." *Id.* at 2:61–63.

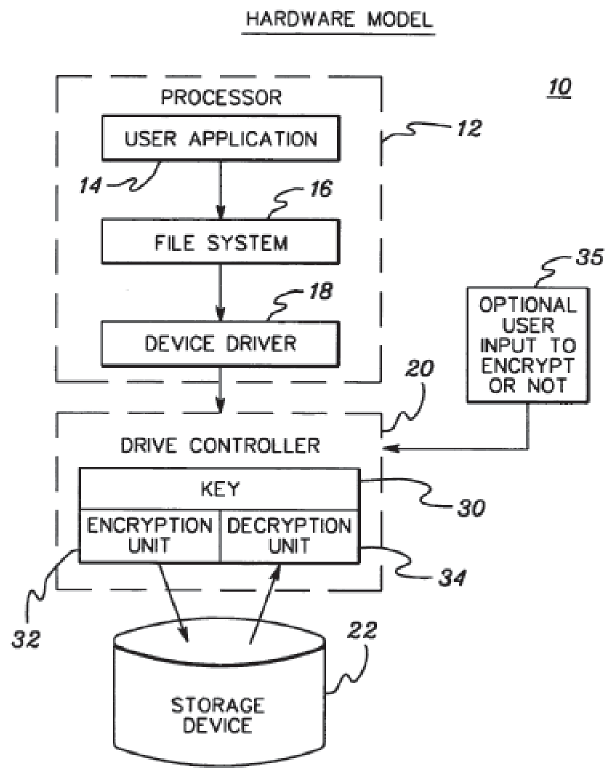


fig. 1

Figure 1 shows computing system 10 with processor 12 and drive controller 20. "The hardware encryption and decryption could be either in the drive controller 20 (as shown), or in the drive itself." *Id.* at 3:50–52. Detrick states driver controller 20 can "regulate the flow of data to and from a disk drive, floppy drive, etc." *Id.* at 3:65–67. Detrick discloses "[c]ommon types of drive controllers include . . . SCSI." *Id.* at 4:1–2.

2. Analysis

Petitioner asserts Figure 1 of Detrick shows encryption/decryption hardware housed within a data generating device. Pet. 48. Petitioner's declarant, Dr. Long, testifies:

> [a] person of ordinary skill in the art at the time of the filing of the '995 Application would have recognized from the teachings of Detrick that the physical security of Nolan's cryptographic

> device (implemented using the SCSI-2 Specification), and particularly access to Nolan's SCSI bus, could be enhanced by housing Nolan's cryptographic device within a data generating device such as a computer.

Id. at 48–49 (quoting Ex. 1006 ¶ 193).

Patent Owner argues again that Nolan and SCSI-2 does not disclose the recited data stream interceptor or main controller, and Hamlin does not supply the missing teaching. PO Resp. 49–50. Similarly, Patent Owner asserts that one of ordinary skill in the art would not place Nolan's apparatus 10 with keyboard and monitor inside a host computer. *Id.* at 49.

For the same reasons discussed above with respect to claims 9 and 14, we agree with Petitioner that the teachings in Nolan and SCSI-2 satisfy the data stream interceptor and main controller limitations recited in claim 15. We also find that Petitioner has explained sufficiently how the combination of Nolan, SCSI-2, and Detrick teach or suggest the remaining limitations of claim 15. Based on the current record, and taking into account Patent Owner's secondary consideration arguments discussed below, we determine Petitioner has demonstrated by a preponderance of the evidence that claim 15 would have been obvious over Nolan, SCSI-2, and Detrick.

G. Secondary Considerations

As discussed above we have determined that: (1) Nolan and SCSI-2 teach or suggest the subject matter recited in claims 1–13; (2) Nolan, SCSI-2, and Hamlin teach or suggest the subject matter recited in claim 14; and (3) Nolan, SCSI-2, and Detrick teach or suggest the subject matter recited in claim 15. Nonetheless, our inquiry continues because Patent Owner argues that secondary considerations in the form of industry praise, commercial

success, copying, and licensing establish the nonobviousness of claims 1–15. PO Resp. 50–59.

Secondary considerations, when present, must always be considered as part of an obviousness inquiry. *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA, Inc.*, 699 F.3d 1340, 1349 (Fed. Cir. 2012). Factual inquiries for an obviousness determination include secondary considerations based on evaluation and crediting of objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Notwithstanding what the teachings of the prior art would have suggested to one with ordinary skill in the art at the time of the patent's invention, the totality of the evidence submitted, including objective evidence of nonobviousness, may lead to a conclusion that the challenged claims would not have been obvious to one with ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Secondary considerations may include any of the following: long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, and praise. *See Graham*, 383 U.S. at 17–18; *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007).

To be relevant, evidence of nonobviousness must be reasonably commensurate in scope with the claimed invention. *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (citing *In re Tiffin*, 448 F.2d 791, 792 (CCPA 1971)); *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998). More fundamentally, to be accorded substantial weight, there must be a nexus between the merits of the claimed invention and the evidence of secondary considerations. *In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). "Nexus" is a legally and factually sufficient connection between the

objective evidence and the claimed invention, such that the objective evidence should be considered in determining nonobviousness. *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988). The burden of showing that there is a nexus lies with the Patent Owner. *Id.*; *see In re Paulsen*, 30 F.3d 1475, 1482 (Fed. Cir. 1994).

1. Industry Praise

Patent Owner argues that its line of encryption ASCIs "X-Wall" products (i.e., X-Wall SE, Enigma, IDE-to-IDE version X-Wall CO, SATA-to-SATA version X-Wall MX, and SATA-to-USB version X-Wall FX) embody the claimed invention of the '995 patent, and have generated industry praise. PO Resp. 52–53 (citing Ex. 2013 ¶ 127). We have reviewed the materials and find that Patent Owner has not established a sufficient nexus between the claimed cryptographic device and the alleged industry praise of Patent Owner's products.

First, Patent Owner asserts that

> Rocstor, a provider of fast, high-capacity data storage and encryption security solutions, describes Enova as "a leading ASIC design engineering company focused on bringing innovative encryption security solutions to market" and praises "Enova's leading-edge hardware based encryption products address the increasing requirement for privacy and confidentiality, satisfying the growing demand for maximum security."

PO Resp. 52 (citing Ex. 2018, 1). Although Exhibit 2018 discusses general features of Patent Owner's X-Wall products, Patent Owner does not identify any praise due to specific elements that are recited in the challenged claims. *See* PO Resp. 52–53; Ex. 2018.

Second, Patent Owner cites a 2002 Computerworld article that allegedly praises Enova's X-Wall SE product. PO Resp. 52. Patent Owner asserts that Computerworld describes the X-Wall SE as sitting "between the PC motherboard and the hard disk, encrypting all data flowing to the hard disk," and the operation of X-Wall SE as "transparent to the user." PO Resp. 52 (citing Ex. 2019, 1; *see* Ex. 2013 ¶ 123, Exs. 2029–2030).

As an initial matter, we do not agree the Computerworld article's description of the X-Wall SE product amounts to praise. Rather, the Computerworld article simply describes the X-Wall SE's: (1) location between the PC motherboard and the hard disk; and (2) operation as transparent. However, the article does not on its face attribute any advantage or benefit to these features. Ex. 2019. Thus, we are not persuaded that Exhibit 2019 provides praise for X-Wall SE. *See Bayer Healthcare Pharms., Inc. v. Watson Pharms., Inc.*, 713 F.3d 1369, 1377 (Fed. Cir. 2013) (finding that brief discussions of Patent Owner's product in journal articles "fall well short of demonstrating true industry praise").

Furthermore, to the extent that the Computerworld article touts advantages of the X-Wall SE product, Patent Owner does not does not explain sufficiently where these product features are recited in the challenged claims. For example, in his Declaration, Dr. Conte describes X-Wall SE as performing transparent encryption, which requires "no special software or changes to the host computer or disk drive." Ex. 2013 ¶ 123 (citing Exs. 2037, 2030). However, Dr. Conte and Patent Owner do not explain how the challenged claims require no special software or changes to the host computer or disk drive. As an example, claim 9 recites "at least one cipher engine adapted to *transparently* encrypt or decrypt at least one data

stream between said at least one data generating device and said at least one data storage device on command from said main controller." Ex. 1001, 6:46–47 (emphasis added). Nonetheless, Patent Owner has not explained sufficiently how transparent operation, as described in the Computerworld article, relates to the recited function of "transparently encrypt or decrypt." Moreover, even assuming the transparent operation discussed in the Computerworld article describes "transparently" encrypting or decrypting, as claimed, Petitioner has demonstrated that this feature, as discussed above, is disclosed by Nolan. *See* Pet. 29–30 (citing Ex. 1006 ¶ 133). Under these circumstances, any evidence of secondary considerations stems from what was known in the prior art, so that there can be no nexus. *Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1369 (Fed. Cir. 2011) ("If [secondary considerations are] due to an element in the prior art, no nexus exists.").

Third, Patent Owner asserts its products embodying the invention of the '995 patent have received industry awards. PO Resp. 52. Patent Owner argues that its Enigma I product received an Editor's Choice Award and an "Excellent" rating from PC Magazine for Enigma I's "[s]imple, seamless full-disk encryption for any USB mass storage device." *Id.* at 52–53 (citing Ex. 2013 ¶ 127; Ex. 2017, 1). Patent Owner also asserts that Enigma I won a TAITRONICS Technology Innovation Award in 2012. *Id.* at 53 (citing Ex. 2013 ¶ 127; Ex. 2015, 1). Additionally, Patent Owner asserts that its X-Wall MX product was awarded a 2012 Business World Golden Bridge Award in the Encryption Solutions Innovations category. PO Resp. 53 (citing Ex. 2020).

Turning first to the PC Magazine award, we do not agree that Patent Owner has established a sufficient nexus between the "Editor's Choice

Award"/"Excellent" rating of Enigma I and the claimed features of the '995 patent. PC Magazine describes several "pros" and "benefits" of Enigma I, including "[s]imple, seamless full-disk encryption for any USB mass storage device." Ex. 2017, 1. Patent Owner attributes the advantage of a "[s]imple, seamless full-disk encryption for any USB mass storage device" to the claimed elements of the '995 patent, but does not explain specifically what claimed features provide this advantage. In his declaration, Dr. Conte testifies that Enigma's encryption is "totally transparent," as it uses the patented methods of the '995 patent. Ex. 2013 ¶ 127. However, Dr. Conte does not indicate how "transparent" encryption relates to the "simple, seamless full-disk encryption" discussed in the PC Magazine article. *Id.* Moreover, even assuming Patent Owner and Dr. Conte attribute "simple, seamless full-disk encryption" to transparent encryption, as claimed, Petitioner has demonstrated that this feature, as discussed above, is disclosed by Nolan. *See* Pet. 29–30 (citing Ex. 1006 ¶ 133).

We also are not persuaded by Patent Owner's reliance on a TAITRONICS Technology Innovation Award given to Enigma I or the Business World Golden Bridge Award for X-Wall MX in 2012. Ex. 2015, 1; Ex. 2020, 6. Exhibit 2015 provides no discussion of the Enigma product other than listing "Enigma" as a product receiving a TAITRONICS award. Ex. 2015, 1. Similarly, for Business World Golden Bridge Award, Exhibit 2020 only lists X-Wall MX without any discussion or description of X-Wall MX. Ex. 2020, 6. As a consequence, we are unable to determine whether the Enigma product or X-Wall MX include features recited in the challenged claims.

Fourth, Patent Owner relies on its previous business relationship with Petitioner and Petitioner's description of Petitioner's own products as evidence of industry praise. PO Resp. 54–56. Patent Owner argues that Petitioner was aware of industry praise for Patent Owner's products and sought out Patent Owner's assistance to bring hardware encryption products to market. *Id*. at 53. Patent Owner further asserts that Petitioner purchased Patent Owner's X-Wall products and used them in Petitioner's hard disk drives, including Petitioner's Momentus drive. *Id.* at 53–55 (citing Ex. 2027 ¶¶ 15–17, Answer to Complaint). According to Patent Owner, by using Patent Owner's products, Petitioner touted and advertised the advantages of hardware-based full disk encryption and transparent encryption. *Id.* at (citing Exs. 2006–2008, 2013 ¶ 127; Ex. 2027 ¶¶ 15–19, 22). Patent Owner further asserts that Petitioner extended the '995 patent's hardware encryption technology to Petitioner's BlackArmor product (*id.* at 56–57), and that "Seagate's chief technologist, Dr. Robert Thibadeau, praised the patented hardware encryption technology Enova provided to Seagate" (*id.* at 54 (citing Ex. 2005, 3–6)).

To start, Patent Owner's assertions are unpersuasive because Patent Owner cites to unsubstantiated allegations made in its Complaint, from the related district court proceeding between the parties, which Petitioner has denied in a responsive Answer. PO Resp. 54–56 (citing Ex. 2005; Ex. 2027). For example, in response to paragraph 17 of the Complaint, Petitioner admitted that it published a press release on June 8, 2005, describing its Momentus drive as having hardware-based full disk encryption, but denied the other allegations of paragraph 17. Ex. 2027 ¶ 17. Patent Owner has not cited to the underlying press release at issue in

paragraph 17, and we decline to comb through the submissions in this proceeding to confirm the presence of the referenced press release in the record and ascertain its contents.

As a further example, Patent Owner argues that Petitioner's statements regarding its "BlackArmor" product apply to claimed elements of the '995 patent. PO Resp. 56–57 (citing Ex. 2021, 1; Ex. 2027 ¶ 25). Presumably, Patent Owner's assertion is based on the allegation that Petitioner's BlackArmor product infringes the '995 patent. Ex. 2005 ¶ 30. Petitioner disputes Patent Owner's allegations (Ex. 2027 ¶ 30) and Patent Owner has not established that the BlackArmor product infringes the '995 patent or incorporates any claimed elements of the '995 patent. Additionally, Patent Owner cites to Exhibit 2021, which shows "BlackAmor" listed as a CES winner. Ex. 2021, 1. But Exhibit 2021 provides no discussion of the BlackAmor product features. Thus, Patent Owner has not established that Black Armor received this award due to the claimed elements of the '995 patent.

Dr. Conte's testimony also does not establish that the allegations made in the Complaint and Answer of the related district court proceeding establish nexus. Dr. Conte relies on unsubstantiated allegations in Patent Owner's Complaint that Dr. Thibadeau praised Patent Owner's patented hardware (Ex. 2005, 3–6); however, Petitioner has denied these allegations (Ex. 2027 ¶ 14). Ex. 2013 ¶ 127. In addition, Dr. Conte confirmed in his cross-examination testimony that he has not analyzed Petitioner's products other than reviewing Petitioner's public statements and taking a photograph of the Momentus drive. Ex. 1029, 118:25–120:11.

Next, we are not persuaded by Patent Owner's contention that Petitioner's own statements regarding hardware-based encryption and transparent encryption establish a nexus for industry praise of claimed elements in the '995 patent. PO Resp. 54–56 (citing Exs. 2006–2008). For example, Patent Owner relies on the testimony of Dr. Conte to assert that Petitioner's statements regarding Petitioner's own Momentus product amount to industry praise of the claimed elements in the '995 patent because the "hardware-based encryption FDE feature" of the Momentus product is accomplished through the claimed limitation of "whether incoming data would be encrypted or passed through based on the received input," and the "transparency" feature of the product is provided by the "cipher engine adapted to transparently encrypt." PO Resp. 55 (citing Ex. 2013 ¶ 127). However, Petitioner's statements discussing its own products (e.g., Momentus) and are not attributed to Patent Owner's encryption products or any claimed element of the '995 patent. Exs. 2007–2008, 2013. Further, as discussed above, Dr. Conte admitted during cross-examination that he has not conducted an analysis of Petitioner's hard disk drive products with encryption beyond considering Petitioner's "public statements" and removing the cover of one of Petitioner's device to take a "picture" of it. Ex. 1029, 118:25–120:11.

With respect to the referenced "picture," we also do not agree that Dr. Conte's "picture" establishes a sufficient nexus. The "picture" is shown as photos at paragraph 127 of Dr. Conte's declaration. Ex. 1029, 118:25–120:2. In one of the photos, we discern a chip bearing the description "Enova X-Wall CO." Ex. 2013 ¶ 127. Dr. Conte testifies that "X-Wall CO is a revised version of the X-Wall SE . . . [and] [l]ike the SE, it practices the

claimed transparent encryption of the ’995 patent.” *Id.* ¶ 124. In describing X-Wall SE, Dr. Conte testifies that it “intercepts IDE data streams and transparently encrypts the data. As it performs the transparent encryption of the invention, it requires no special software or changes to the host computer or disk drive.” *Id.* ¶ 123 (citing Ex. 2030, 2; Ex. 2037, 3). Dr. Conte’s descriptions of both X-Wall SE and X-Wall CO do not explain how the challenged claims recite performing transparent encryption with “no special software or changes to the host computer or disk drive.” Ex. 2013 ¶¶ 123–124.

Moreover, even assuming that Petitioner’s statements are attributable to claimed elements of hardware-based encryption and transparency, Petitioner has demonstrated that these elements are disclosed in Nolan and SCSI-2, as discussed above. Indeed, the ’995 patent itself acknowledges that hardware-based encryption was known and conventional as of the filing date. Ex. 1001, 1:35–40. In addition, to the extent that Patent Owner asserts that there is a difference between hardware-based encryption and hardware-based *full disc* encryption, Patent Owner and Dr. Conte have not explained sufficiently how such a difference establishes a nexus between Petitioner’s Momentus product and the claimed invention of the ’995 patent. For example, Petitioner’s presentation shown in Ex. 2007 describes several features of full disc encryption including: (1) a closed encryption device for which encryption cannot be turned off (*id.* at 3); (2) FDE functionality (*id.* at 6); and (3) “FDE Keys and IDs” (*id.* at 7). However, Patent Owner has not explained sufficiently what aspects of full disc encryption are tied to the claimed elements of the ’995 patent. *See, e.g.*, Ex. 2007, 1–12.

Accordingly, based on the entire record, we determine that Patent Owner has not established a sufficient nexus between the merits of the claimed invention and industry praise of either Patent Owner's products or Petitioner's products.

2. Commercial Success

As evidence of commercial success, Patent Owner relies on its previous business relationship with Petitioner and Petitioner's alleged praise and advertisement of Patent Owner's encryption devices. PO Resp. 53–57. For the same reasons discussed above, we are not persuaded Patent Owner has established a sufficient nexus between the merits of the claimed invention and either Patent Owner's own products or Petitioner's products.

In addition, we are not persuaded by Patent Owner's arguments regarding the sales of Petitioner's products constitute evidence of commercial success. PO Resp. 56–57. Patent Owner asserts that: (1) Petitioner's "efforts to bring its FDE drives to market were successful because of Enova's key technological assistance and supply of X-Wall ASICs"; (2) "[i]n February 2011, Seagate 'announced that it has shipped more than 1 million self-encrypting laptop and enterprise hard drives'"; and (3) "Seagate further explained that '[s]ales of the Seagate® hard drives with built-in encryption continue to surge as more computer makers offer the drives to protect against unauthorized access to sensitive data.'" *Id.* at 56–57 (citing Ex. 2009, 1; Ex. 2027 ¶ 26).

Initially, we note "[e]vidence of commercial success, or other secondary considerations, is only significant if there is a nexus between the claimed invention and the commercial success." *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1311–12 (Fed. Cir. 2006). To show how

commercial success supports nonobviousness, Patent Owner must prove that the sales were a direct result of the unique characteristics of the invention, and not a result of economic and commercial factors unrelated to the quality of the patented subject matter. *In re Applied Materials, Inc.*, 692 F.3d 1289, 1299–1300 (Fed. Cir. 2012). In addition, "if the commercial success is due to an unclaimed feature of the device," or "if the feature that creates the commercial success was known in the prior art, the success is not pertinent." *Ormco*, 463 F.3d at 1312; *see also Huai-Hung Kao*, 639 F.3d at 1070 (requiring a determination of "whether the commercial success of the embodying product resulted from the merits of the claimed invention as opposed to the prior art or other extrinsic factors").

Here, Patent Owner fails to provide sufficient proof of such a relationship between any alleged sales and the unique characteristics of the invention embodied in the challenged claims. First, Patent Owner has not established that the products described in Petitioner's statements include features claimed in the '995 patent. PO Resp. 56–57. Patent Owner simply relies on allegations made in the Complaint of the related district court proceeding, which, as we explained above, Petitioner has denied. *Id.; see also* Ex. 2027 ¶ 27 (denying infringement of the '995 patent). Further, Petitioner's statements in Exhibit 2009 also do not establish that the sales of Petitioner's "self-encrypting laptop and enterprise hard drives" have any relationship to the merits of the claimed invention. Additionally, Dr. Conte admitted that he did not conduct any economic analysis of either Patent Owner's products or Petitioner's products. Ex. 1029, 115:24–118:12; 120:13–25; 121:9–122:1.

Moreover, even if the Petitioner's product sales are considered in the context of commercial success, "evidence related solely to the number of units sold provides a very weak showing of commercial success, if any." *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996). According to the Federal Circuit, "the more probative evidence of commercial success relates to whether the sales represent 'a substantial quantity in th[e] market.'" *Applied Materials*, 692 F.3d at 1300 (quoting *Huang*, 100 F.3d at 140). Patent Owner offers no evidence of the size of the market to which to compare Petitioner's sales. Accordingly, we are not persuaded that Patent Owner's alleged objective indicia of commercial success shows non-obviousness.

3. Copying and Licensing

Patent Owner further argues that copying and licensing of the '995 patent by others is objective indicia of non-obviousness. Specifically, Patent Owner argues that Initio Corporation ("Initio") marketed and sold infringing products incorporating the patented invention of the '995 patent to major hard drive manufactures. PO Resp. 57–58 (citing Ex. 2004; Ex. 2032). Patent Owner contends the resolution of *Enova v. WD* "confirms Initio's infringement of the '995 patent" because "Initio admitted in a consent judgment that its products practice the '995 patent and further began marking its products with the '995 patent number." *Id.* at 58 (citing Ex. 2004, 2). Patent Owner additionally argues that Western Digital and Buffalo, Inc. each incorporated Initio encryption circuits in their hard drives, and that both parties entered agreements with Patent Owner to resolve their disputes in *Enova v. WD*. *Id.* at 58–59 (citing Ex. 2024; Ex. 2042–45). Patent Owner adds that both Initio and Western Digital license the '995 patent from Patent Owner.

Patent Owner's reliance on Initio's consent judgement in *Enova v. WD* does not establish that Initio copied the claimed invention or infringed the '995 patent based on the unique aspects of the claimed subject matter. It is not sufficient that a product or its use merely be within the scope of a claim in order for objective evidence of nonobviousness tied to that product or use to be given substantial weight. Like other types of objective evidence, evidence of copying must be shown to have nexus. *Wm. Wrigley Jr. Co. v. Cadbury Adams USA LLC*, 683 F.3d 1356, 1364 (Fed. Cir. 2012). Moreover, a showing of copying is only equivocal evidence of nonobviousness in the absence of more compelling objective indicia of other secondary considerations. *Ecolochem, Inc. v. S. Cal. Edison Co.*, 227 F.3d 1361, 1380 (Fed. Cir. 2000). Copying could result from lack of concern about patent property, contempt for the patent, or accepted practices in the industry, among others. *Cable Elec. Prods., Inc. v. Genmark, Inc.*, 770 F.2d 1015, 1028 (Fed. Cir. 1985), *overruled on other grounds by Midwest Indus., Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356, 1359 (Fed. Cir. 1999).

We also are not persuaded by Patent Owner's arguments regarding licensing and settlement. Patent Owner relies on Exhibits 2042, 2043, and 2044. These exhibits are almost entirely redacted. In fact, they are redacted to the point that even the parties involved in the agreements have been obscured. Exs. 2042–44; Tr. 70:21–71:8. Thus, because we cannot verify Patent Owner's assertions regarding these agreements, we find that these agreements do not provide objective evidence of nonobviousness.

4. Summary

Accordingly, on balance, we determine that Petitioner's strong evidence of obviousness, which includes that claims 1–13 would have been

obvious based on Nolan and SCSI-2; claim 14 would have been obvious based on Nolan, SCSI-2, and Hamlin; and claim 15 would have been obvious based on Nolan, SCSI-2, and Detrick, under 35 U.S.C. § 103(a), outweighs the evidence of secondary considerations of nonobviousness submitted by Patent Owner,

H. Petitioner's Motion to Exclude

Petitioner seeks to exclude Exhibits 2004–2009, 2015, 2017–2032, 2037–2047, and paragraphs 117–130 of Exhibit 2013. Pet. Mot. Exclude 1. In particular, Petitioner argues that Patent Owner "has failed to establish the nexus necessary to show the relevance of this evidence." *Id.* at 1–13. We need not reach the merits of Petitioner's Motion to Exclude because, as explained above, even if the disputed evidence is considered, Patent Owner has not shown that the evidence of secondary considerations of nonobviousness it submitted outweighs the strong evidence of obviousness presented by Petitioner. Accordingly, Petitioner's Motion to Exclude is *dismissed as moot*.

I. Patent Owner's Motion to Exclude

Patent Owner asserts that Petitioner's reliance on Exhibit 1028 in Petitioner's Reply improperly adds a new reference and new basis to Petitioner's obviousness challenges presented in the Petition and discussed in the Board's Decision to Institute. PO Mot. to Exclude 1–7. Patent Owner seeks to exclude Exhibit 1028 because it asserts Petitioner was required to present Exhibit 1028 earlier in the proceeding. *Id.* We do not rely on the disputed evidence in rendering this Final Written Decision. Therefore, Patent Owner's Motion to Exclude is *dismissed as moot*.

J. Patent Owner's Motion to Seal

Patent Owner filed a Motion to Seal Exhibits 2042, 2043, and 2044 under 37 C.F.R. § 42.54. Paper 23. In its Motion, Patent Owner asserts that the redacted exhibits are "confidential" agreements reached between the Patent Owner and third parties Initio, Western Digital, and Buffalo, Inc., each of which are not involved in this proceeding. Mot. to Seal 1. With its Motion to Seal, Patent Owner filed confidential redacted versions of Exhibits 2042, 2043, and 2044, but did not file confidential unredacted copies of the same. Patent Owner indicated that it intended to file unredacted versions of the agreements, but had not received the consent of the third parties to do so. Mot. to Seal 2; *See* Tr. 70:21–71:7.

The standard for granting a motion to seal is "for good cause." 37 C.F.R. § 42.54. Patent Owner, as the moving party, has the burden of proof in showing entitlement to the requested relief. 37 C.F.R. § 42.20(c). We need to know why the information sought to be sealed constitutes the Patent Owner's confidential information.

In reviewing the "confidential" version of these exhibits, we note that each exhibit has been heavily redacted, leaving only a handful of lines per each exhibit. As we explained in the oral hearing, these unredacted portions do not provide sufficient detail to verify the contents of these exhibits. *See, e.g.*, Tr. 70:21–71:7. Thus, we cannot confirm Patent Owner's assertions regarding the confidentiality of these exhibits, nor can we grant Patent Owner's Motion to Seal for good cause. Accordingly, we deny Patent Owner's Motion to Seal Exhibits 2042, 2043, and 2044.

Additionally, Patent Owner has submitted a revised proposed protective order (Ex. 2049) that reflects the terms of a protective order

entered in the parties' co-pending district court proceeding. Mot. to Seal 3. Patent Owner represents that it has conferred with Petitioner regarding the terms of the proposed protective order; however, no agreement has been made. *Id.*

We note that the Office Patent Trial Practice Guide states the following concerning protective orders:

> (a) Purpose. This document provides guidance on the procedures for filing of motions to seal and the entry of protective orders in proceedings before the Board. The protective order governs the protection of confidential information contained in documents, discovery, or testimony adduced, exchanged, or filed with the Board. The parties are encouraged to agree on the entry of a stipulated protective order. *Absent such agreement, the default standing protective order will be automatically entered.*

Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48769 (Aug. 14, 2012) (App'x B (emphasis added)). As we cannot ascertain that the contents of the redacted Exhibits 2042, 2043, and 2044 constitute the Patent Owner's confidential information, we do not grant Patent Owner's request to enter its proposed protective order. We do, however, enter the default Protective Order provided in Appendix B of the Trial Practice Guide.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–15 of the '995 patent are held unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed as moot*;

FURTHER ORDERED that Petitioner's Motion to Exclude is *dismissed as moot*;

FURTHER ORDERED that Petitioner's Motion to Seal is *denied*;

FURTHER ORDERED that the Board's default Protective Order appearing in the Office Trial Practice Guide, 77 Fed. Reg. 48,756, 48,769–71 (Aug. 14, 2012), is hereby *entered* in this proceeding; and

FURTHER ORDERED that any party to the proceeding seeking judicial review of this Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Richard M. Marsh, Jr.
Faegre Baker Daniels LLP
richard.marsh@faegreBD.com

Elizabeth Cowan Wright
Faegre Baker Daniels LLP
elizabeth.cowanwright@faegreBD.com

Christopher L. Larson
Faegre Baker Daniels LLP
chris.larson@faegreBD.com

Calvin L. Litsey
Faegre Baker Daniels LLP
calvin.litsey@faegreBD.com

David J.F. Gross
Faegre Baker Daniels LLP
david.gross@faegreBD.com

PATENT OWNER:

Hector Ribera
Fenwick & West LLP
hribera@fenwick.com

Robert Hulse
Fenwick & West LLP
rhulse@fenwick.com

Natu J. Patel
The Patel Law Firm, P.C.
npatel@thepatellawfirm.com

Trials@uspto.gov
571-272-7822

Paper 10
Entered: October 2, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SEAGATE TECHNOLOGY (US) HOLDINGS, INC., and
SEAGATE TECHNOLOGY LLC,
Petitioner,

v.

ENOVA TECHNOLOGY CORP.,
Patent Owner.

Case IPR2014–00683
Patent 7,136,995 B1

Before MICHAEL R. ZECHER, GEORGIANNA W. BRADEN, and FRANCES L. IPPOLITO, *Administrative Patent Judges.*

IPPOLITO, *Administrative Patent Judge.*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Seagate Technology (US) Holdings, Inc. and Seagate Technology LLC (collectively "Petitioner") filed a Corrected Petition ("Pet.") requesting an *inter partes* review of claims 1–15 of U.S. Patent No. 7,136,995 B1 ("the '995 patent"). Paper 4. Patent Owner Enova Technology Corp. timely filed a Preliminary Response ("Prelim. Resp.") to the Petition. Paper 9. We have jurisdiction under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a):

> THRESHOLD.—The Director may not authorize an *inter partes* review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

Pursuant to 35 U.S.C. § 314, we conclude there is a reasonable likelihood Petitioner would prevail with respect to claims 1–15.

A. Related Proceedings

Petitioner indicates the '995 patent currently is the subject of a related proceeding between the parties in the U.S. District Court for the District of Delaware, No. 1:13-cv-1011-LPS, which was filed on June 5, 2013. Pet. 1. Petitioner also indicates the '995 patent was the subject of prior federal district court proceeding in the U.S. District Court for the District of Delaware, No. 1:10-cv-00004-LPS ("*Enova v. WD*"), which closed on March 4, 2013. *Id.* Additionally, related U.S. Patent No. 7,900,057 B2 is the subject of the petition for *inter partes* review in Cases IPR2014–01178, IPR2014-01297, and IPR2014-01449.

B. The ’995 Patent

The ’995 patent describes a cryptographic device that performs encryption/decryption during data transfers between a data generating device and a data storage device. Ex. 1001, 3:22–24. Figure 4 (reproduced below) depicts schematically the architecture of cryptographic device 43 described in the ’995 patent. *Id*. at 4:30–32.

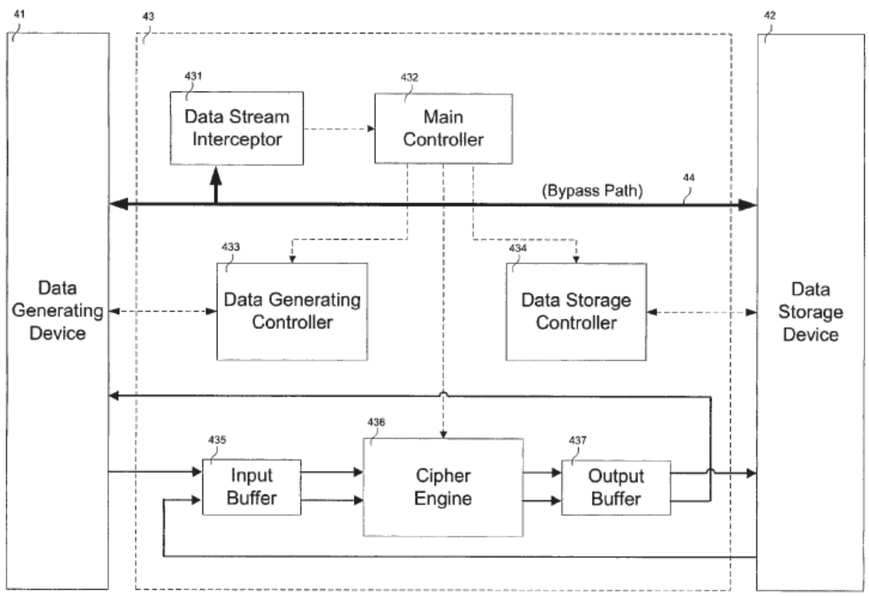


FIG. 4

Figure 4 shows cryptographic device 43 operatively coupled between data generating device 41 and data storage device 42 for use during data transfer. *Id.* at 4:32–35. The ’995 patent indicates that data generating device 41 may be “a desktop/notebook computer, microprocessor . . . or any other device capable of generating data.” *Id.* at 4:36–38. The ’995 patent adds that data storage device 42 may be “a computer hard drive, tape drive . . . magnetic tape . . . or any other device capable of storing data for retrieval purposes.” *Id.* at 4:38–44. Further, crytographic device 43 is described as adapted to “perform transparently data encryption and decryption during

data transfers between data generating device 41 and data storage device 42 with no impact on overall system performance." *Id.* at 4:45–49.

Additionally, Figure 4 shows that cryptographic device 43 includes data stream interceptor 431 operatively coupled to a main controller 432. Ex. 1001, 4:50–52. Main controller 432 communicates control signals to data generating controller 433, data storage controller 434, and cipher engine 436. *Id.* at 4:52–54. Main controller 432 receives input from data stream interceptor 431 and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, decrypted or passed through unmodified. *Id.* at 4:55–58. The '995 patent discloses that data stream interceptor 431 is adapted to distinguish between command/control and data signal transfers, and is configured to pass through certain command/control signals via bypass data path 44, and intercept other command/control signals which are transmitted to main controller 432. *Id.* at 4:58–65. Main controller 432 also "instructs data generating controller 433 and data storage controller 434 to perform specific data transfer protocols . . . of data generating device 41 and data storage device 42, respectively, according to the intercepted command/control signals." *Id.* at 4:65–5:4.

As discussed previously, Figure 4 shows cipher engine 436. "Main controller 432 also transmits control signals to cipher engine 436 to notify the same of an incoming data stream." Ex. 1001, 5:4–6. Cipher engine 436 is programmed to transparently encrypt/decrypt streaming data during data transfer between data generating device 41 and data storage device 42. *Id.* at 5:6–11.

C. Illustrative Claim

Of the challenged claims, claims 1, 5, 9, 13, 14, and 15 are independent. Claim 9 is illustrative of the subject matter of the ’995 patent, and is reproduced below:

> 9. A cryptographic device, comprising:
>
> at least one data stream interceptor that distinguishes between command/control and data signal transfers;
>
> a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;
>
> at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;
>
> at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and
>
> at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

Ex. 1001: 6:45–64.

D. The Prior Art

Petitioner relies on the following prior art:

Reference	Patent/Printed Publication	Publication Date	Exhibit
Nolan	GB Patent App. No. 2,264,373 A	Aug. 25, 1993	Ex. 1002
SCSI-2	ANSI X3.131-1994 (R1999), *Small Computer System Interface-2*	1994	Ex. 1003
Hamlin	US Patent No. 6,735,693 B1	May 11, 2004	Ex. 1004
Detrick	US Patent No. 7,278,016 B1	Oct. 2, 2007	Ex. 1005

E. The Asserted Grounds[1]

Petitioner asserts that the challenged claims are unpatentable based on the following grounds:

Reference[s]	Basis	Claim(s) Challenged
Nolan and SCSI-2	§ 103	1–13
Nolan and SCSI-2	§ 103	14 and 15
Nolan, SCSI-2, and Hamlin	§ 103	14
Nolan, SCSI-2, and Detrick	§ 103	15

[1]Petitioner argues claim 14 is unpatentable over the combination of Nolan and SCSI-2, or, alternatively, Nolan, SCSI-2, and Hamlin. Pet. 9. Petitioner further argues claim 15 is unpatentable over the combination of Nolan and SCSI-2, or, alternatively, Nolan, SCSI-2, and Detrick. *Id.* As shown in the table, we treat these respective arguments for claims 14 and 15 as three separate and distinct grounds of unpatentability.

II. ANALYSIS

In the analysis that follows, we discuss facts as they have been presented thus far in this proceeding. Any inferences or conclusions drawn from those facts are neither final nor dispositive of any issue related to any ground on which we institute review.

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the Specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). Under the broadest reasonable construction standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Neither Petitioner nor Patent Owner contends that any special definition has been provided in the specification for any claim term. We conclude the same.

For the purposes of this decision, we construe the claim terms as follows below.

1. data stream interceptor that distinguishes between command/control and data signal transfers (claims 1, 5, 9, and 13–15)

Petitioner asserts that the broadest reasonable construction of the phrase "data stream interceptor that distinguishes between command/control and data signal transfers" is "one or more components adapted to intercept at least one data stream and distinguish the command or control signals *in the*

data stream from the data signals." Pet. 10 (emphasis added) (citing Ex. 1001, 4:55–65; Ex. 1006 ¶ 92). Patent Owner proposes a different and broader construction of "one or more components adapted to intercept at least one data stream and distinguish between command/control signal transfers and data signal transfers." Prelim. Resp. 10–11 (citing Ex. 2001, 7).

Based on the current record, we are persuaded that Petitioner's proposal is consistent with the Specification, which discloses that cryptographic device 43 is coupled between data generating device 41 and data storage device 42 *for use during data transfer*. Ex. 1001, 4:32–35 (emphasis added). The Specification further discloses that main controller 432 of cryptographic device 43 receives input from data stream interceptor 431 and determines "whether *an incoming data stream* . . . is to be encrypted, decrypted or passed through." *Id.* at 4:55–58 (emphasis added). The Specification goes on to disclose that "*[i]n this regard*, data stream interceptor 431 is adapted to distinguish between command/control and data signal transfers." *Id.* at 4:58–60 (emphasis added). Thus, for purposes of this decision, we adopt Petitioner's construction of the phrase "data stream interceptor that distinguishes between command/control and data signal transfers" because we are persuaded that it is the broadest reasonable construction in light of the Specification of the '995 patent.

2. at least one cipher engine adapted to transparently encrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller (claim 1);

at least one cipher engine adapted to transparently decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller (claim 5);

at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller (claim 9); and

a cipher engine adapted to transparently encrypt or decrypt at least one data stream between the data generating device and the data storage device on command from said main controller (claims 13–15).

Referring to claims 1, 5, 9, and 13–15, Petitioner proposes that the phrase "cipher engine adapted to transparently [encrypt or decrypt] at least one data stream between . . . generating device and . . . data storage device on command from said main controller" means

> one or more components adapted to encrypt or decrypt at least one data stream between a data generating device and a data storage device on command from the main controller *without using resources during data transfers that are typically associated with either the data generating device or the data storage device*.

Pet. 11–12 (emphasis added) (citing Ex. 1001, 3:22–34, 3:62–4:2, 4:21–29, 5:4–11; Ex. 1006 ¶ 92). As part of this proposal, Petitioner construes "transparently" to mean "without using resources during data transfers that are typically associated with either the data generating device or the data storage device." Patent Owner proposes that "transparently" means "functionally, data transfers appear to be performed directly between the data generating device and data storage device." Prelim. Resp. 13–14

(Ex. 2001, 8; Ex. 2002, 1).

For the purposes of this decision, we find it necessary only to construe the term "transparently," without express construction of the other terms recited in the cipher engine limitations of claims 1, 5, 9, and 13–15. Looking to the Specification, it does not expressly define "transparently." Under such circumstances, "in determining the ordinary and customary meaning of the claim term as viewed by a person of ordinary skill in the art, it is appropriate to consult a general dictionary definition of the word for guidance." *Comaper Corp. v. Antec, Inc.*, 596 F.3d 1343, 1348 (Fed. Cir. 2010) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1322–23 (Fed. Cir. 2005) (en banc). One dictionary, the Microsoft Computer Dictionary (1997), defines "transparent" as "[i]n computer use, of, pertaining to, or characteristic of a device, function, or part of a program that works so smoothly and easily that it is invisible to the user." Ex. 3001, 3. This definition is consistent with the Specification, which discloses, "[i]n general the cryptographic device acts as an 'invisible' data transfer bridge connecting data generating device 13 and data storage device 11." Ex. 1001, 3:34–36 (emphasis omitted).

Furthermore, we note the constructions offered by Petitioner and Patent Owner are more restrictive than the claim language, which does not recite explicitly that (1) encryption or decryption is performed without using resources associated with data generating or storage devices, or (2) data transfers appear to be performed directly between the data generating device and data storage device. Thus, based on the current record, we construe "transparently" to mean "functionally invisible" because this construction is consistent with the ordinary and customary meaning of "transparent" as

would be understood by one with ordinary skill in the art in light of the ’995 patent.

> 3. *a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted or passed through based on the received input from said at least one data stream interceptor (claim 1);*
>
> *a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be decrypted or passed through based on the received input from said at least one data stream interceptor (claim 5);*
>
> *main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor (claims 9 and 13); and*
>
> *a main controller receiving input from said data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor (claims 14 and 15)*

Petitioner argues that the broadest reasonable construction of these similar claim phrases is “one or more components adapted to receive input from the data stream interceptor and determine whether an incoming data stream is to be encrypted, decrypted or passed through based on input received from the data stream interceptor.” Pet. 10 (citing Ex. 1001, 4:55–58; Ex. 1006 ¶ 92). Petitioner notes that the claim phrases differ between the challenged claims in whether “encrypted,” “decrypted,” or “encrypted, decrypted” is recited. *Id.* at n.2. In response, Patent Owner proposes constructions for “main controller,” “encrypted,” “input,” and “passed through.” Prelim. Resp. 11–12 (citing Ex. 2002, 1–2; Ex. 2001, 5, 6). For

the purposes of this decision, we need only construe the term "input." For the term "input," Patent Owner proposes the construction of

> main controller receives *input distinguishing between command/control and data signal transfers from the data stream interceptor* and uses that input to determine whether to encrypt/decrypt or pass through each signal.

Id. (emphasis added).

Turning to the Specification, the '995 patent discloses, "[m]ain controller 432 receives input from data stream interceptor 431 and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, decrypted or passed through unmodified." Ex. 1001, 4:55–58. The Specification does not limit the described input to a specific type of information such as that which distinguishes between signals. Thus, Patent Owner's proposed construction is too narrow and excludes embodiments described in the Specification. Based on the current record, we conclude that the term "input," recited in the challenged claims, does not require input distinguishing between command/control and data signal transfers, but rather encompasses either command/control or data signals.

4. *"A cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer" (claim 13);*

   A cryptographic device integrated within a data storage device for use during data transfer with a data generating device (claim 14); and

   A cryptographic device integrated within a data generating device for use during data transfer with a data storage device (claim 15).

Petitioner proposes that the preambles for claims 13, 14, and 15 be construed as follows, respectively

> a cryptographic device situated between and able to transfer data to and from a data generating device and a data storage device;
>
> a cryptographic device housed within a data storage device and able to transfer data to and from a data generating device; and
>
> a cryptographic device housed within a data generating device and able to transfer data to and from a data storage device.

Pet. 12–13 (citing Ex. 1001, 2:34–41, 57–59, 3:34–37, 44–53, 4:3–12; Ex. 1006 ¶ 92). We understand Petitioner's position to be that the preambles of claims 13, 14, and 15 are entitled to patentable weight. Patent Owner does not provide a construction for these terms. Prelim. Resp. 15–16.

In general, a preamble is construed as a limitation "if it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim." *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (quotations and citations omitted). Here, the preambles in claim 13, 14, and 15 all provide antecedent basis for the "data storage device" and "data generating device," which are later recited in the body of the claims. Moreover, the language of the limitations recited in the body of claims 13, 14, and 15 are essentially identical. Thus, the preambles, which indicate the location of the cryptographic device, provide the only difference in claim scope between claims 13, 14, and 15. Based on the current record, we conclude the preambles are essential to understand the scope of claims 13, 14, and 15, and operate as claim limitations. *See id*. (finding that the preamble constitutes a limitation when the claim depends on it for antecedent basis, or when it "is essential to understand limitations or terms in claim body.") Other terms in the preambles need not be construed expressly for purposes of this decision.

5. Other Terms

Petitioner proposes constructions for the following phrases: (1) "data generating controller adapted to perform at least one data transfer protocol with . . . data generating device on command from said main controller"; (2) "data storage controller adapted to perform at least one data transfer protocol with . . . data storage device on command from said main controller"; and (3) "wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer." Pet. 11–12. We cannot discern how Petitioner's constructions add any clarity to each of the phrases, which are each relatively simple to understand. Thus, we need not construe expressly these terms at this stage. Additionally, all other claim terms need not be construed expressly for purposes of this decision.

B. Claims 1–13 – Obviousness over Nolan (Ex. 1002) and SCSI-2 (Ex. 1003)

Petitioner argues claims 1–13 are unpatentable under 35 U.S.C. § 103(a) over Nolan and SCSI-2. Pet. 15–40. As explained below, we have considered the arguments and evidence presented, and we are persuaded there is a reasonable likelihood Petitioner would prevail on its assertion that claims 1–13 are unpatentable over Nolan and SCSI-2.

1. Summary of Nolan (Ex. 1002)

Nolan describes an apparatus for encrypting computer data before storage. Ex. 1002, 1:1–2. Figure 1 (reproduced below) shows a block diagram of an apparatus for encryption that is designed for use with tape drives that use a Small Computer System Interface (SCSI). *Id.* at 4:8–10, 13–15.

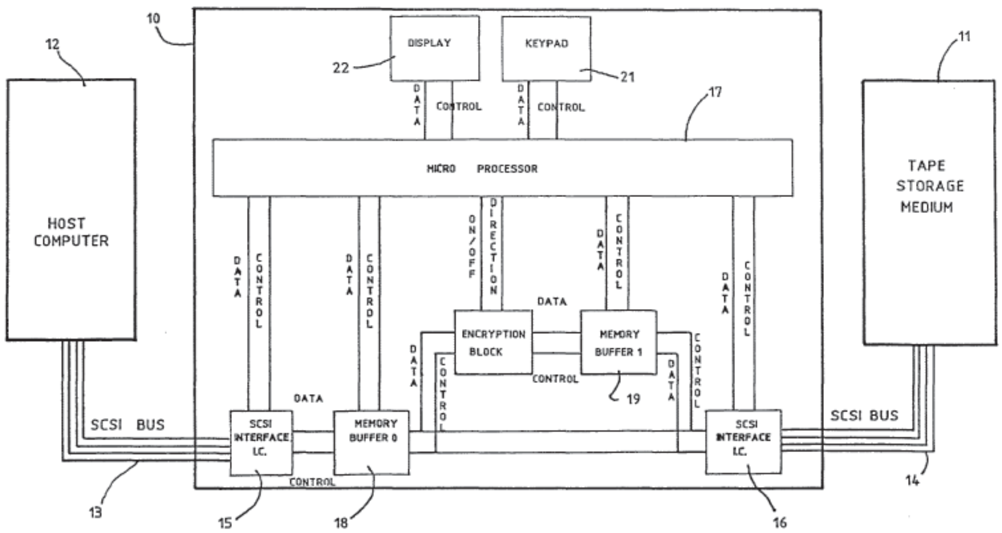


FIG 1

Figure 1 shows encryption/decryption apparatus 10 connected to host computer 12 and tape storage medium 11 via a SCSI BUS. Encryption and decryption apparatus 10 includes host computer interface 15 and tape drive interface 16 on respective sides. Ex. 1002, 4:25–26.

Encryption/decryption apparatus 10 includes an encryption block and microprocessor 17. Under the control of the microprocessor 17, host computer interface 15, tape drive interface 16, and the encryption block transfer data to or from host memory buffer 18 or target memory buffer 19. *Id.* at 4:27–5:8. Whether a particular memory block responds to a request signal is controlled by microprocessor 17. Microprocessor 17 can switch on and off the flow of data into and out of a particular memory buffer from a particular source or destination. *Id.* at 5:13–18. Microprocessor 17 also sets the encryption block to encrypt or decrypt and transfers data through the encryption block from a memory buffer. *Id.* at 5:25–6:2.

Additionally, Nolan's Figure 2 shows a flow diagram of the main program steps performed by microprocessor 17. *Id.* at 6:12–13. After

initiation 30 and 31, microprocessor 17 reads the common encryption key stored on the tape and stores it in unit 10. Ex. 1002, 6:14–16. "[M]icroprocessor 17 waits for a command to be sent from the host computer, step 32" ("Wait for Input SCSI Command"). *Id.* at 6:17–18. If the command involves tape movement, "the anticipated amount of movement is calculated and stored, step 35." *Id.* at 6:21–23. "The microprocessor then ascertains whether any transfer of encrypted data is required, steps 36 and 37." *Id.* at 6:23–25. "If not, the command is executed, step 38." *Id.* "If it does involve the transfer of encrypted data then the stored encryption key is modified by the current tape position, step 39." *Id.* at 6:25–29.

2. Summary of SCSI-2 (Ex. 1003)

SCSI-2 describes SCSI as a local input/output ("I/O") bus that can be operated over a wide range of data rates. Ex. 1003, 35.[2] "When two SCSI devices communicate on the SCSI bus, one acts as an initiator and the other acts as a target. The initiator originates an operation and the target performs the operation." *Id.* at 59.

SCSI-2 discloses that the SCSI architecture includes eight distinct phases: (a) BUS Free phase, (b) ARBITRATION phase, (c) SELECTION phase, (d) RESELECTION phase, (e) COMMAND phase, (f) DATA phase, (g) STATUS phase, and (h) MESSAGE phase. Ex. 1003, 68. SCSI-2 adds that the SCSI bus "can never be in more than one phase at any given time." *Id.* SCSI-2 also refers to the COMMAND, DATA, STATUS, and MESSAGE phases, collectively, as information transfer phases because

[2] All page numbers for SCSI-2 refer to the page number located in the bottom, right-hand corner.

"they are all used to transfer data or control information via the DATA BUS." Ex. 1003, 71.

SCSI-2 also discloses that SCSI bus signals include an I/O signal, a C/D (CONTROL/DATA) signal, and a MSG (MESSAGE) signal. Ex. 1003, 61. The C/D signal is "driven by a target that indicates whether CONTROL or DATA information is on the DATA BUS. True indicates CONTROL." *Id.* SCSI-2 further discloses "[e]ach signal driven by an SCSI device shall have" a lower voltage of 0 to 0.5 volts for signal assertion and a higher level voltage of 2.5 to 5.25 volts for signal negation. *Id.* at 54. Additionally, the C/D, I/O and MSG signals are used to distinguish between the different information transfer phases. *Id.* at 71. The "target drives these three signals and therefore controls all changes from one phase to another." *Id.* Table 8 (reproduced below) shows the use of C/D, I/O, and MSG signals. *Id.* at 72.

Table 8 - Information transfer phases

Signal			Phase name	Direction of transfer		Comment
MSG	C/D	I/O				
0	0	0	DATA OUT	Initiator to target	\	Data
0	0	1	DATA IN	Initiator from target	/	phase
0	1	0	COMMAND	Initiator to target		
0	1	1	STATUS	Initiator from target		
1	0	0	*			
1	0	1	*			
1	1	0	MESSAGE OUT	Initiator to target	\	Message
1	1	1	MESSAGE IN	Initiator from target	/	phase
Key: 0 = False, 1 = True, * = Reserved for future standardization						

As shown in Table 8, during the DATA phase, the C/D signal indicates False. *Id*. During the COMMAND phase, the C/D signal indicates True. *Id.*

3. Analysis

Below we discuss independent claim 9, which is illustrative of claims 1–8 and 10–13.

Claim 9 recites a cryptographic device comprising "at least one data stream interceptor that distinguishes between command/control and data signal transfers." Ex. 1001, 6:46–47. Petitioner asserts that Nolan's disclosure of SCSI Interface 15 implemented using the details of SCSI-2 satisfies this limitation. Pet. 19. More particularly, Petitioner points to Figure 1 of Nolan to show all data streams originating from host computer 12 travel over SCSI bus 13 and are intercepted by SCSI Interface 15 when entering encryption/decryption apparatus 10. *Id.* Petitioner further argues Nolan's SCSI Interface 15 distinguishes between command/control signals and data signals by using the C/D signal disclosed in SCSI-2. *Id.* at 20.

Additionally, Petitioner asserts a person of ordinary skill in the art would have been motivated to combine Nolan's cryptographic device with SCSI-2, because Nolan explicitly teaches the use of SCSI to transfer data between the host computer and the storage medium. Pet. 17. (Citing Ex. 1002, 4:13–15). Petitioner's declarant, Dr. Long, also testifies that:

> The embodiment in Figure 1 of Nolan is implemented using multiple "SCSI bus[es]" and "SCSI Interface[s]" 15 and 16. (*Id.* at Figure 2.) The specification repeats that Nolan can be implemented using "SCSI commands" (see Figure 2) and other features detailed in the "SCSI-1 and SCSI-2" protocols (*id.* at 8:25). In my opinion, these teachings would have directed one of ordinary skill to look to the SCSI-2 Specification for specific details of how the SCSI protocol operates in Nolan.

Ex. 1006 ¶ 58.

Patent Owner first contends Nolan is cumulative of U.S. Patent No. 6,081,895 ("Harrison"), which was prior art of record during prosecution of

the ’995 patent. Prelim. Resp. 23. Patent Owner argues Nolan does not demonstrate any new grounds for *inter partes* review, because Harrison was found by the Examiner to be insufficient to describe a data stream interceptor that distinguishes between command/control and data signal transfers. *Id.* at 26. Patent Owner further argues Nolan and Harrison both show “a box in a diagram and language which indicates that data flows through that box,” and “[e]ach fails to show the details of the operation actually claimed.” Prelim. Resp. 24.

Patent Owner’s arguments are not persuasive because Petitioner does not rely solely on Nolan to teach the recited data stream interceptor. Rather, as we explained above, Petitioner relies on SCSI-2 for the details on implementing Nolan’s SCSI Interface 15. Pet. 19. Furthermore, even if we assume Nolan is cumulative of Harrison, we note that 35 U.S.C. § 325(d) states the following (emphasis added): “In determining whether to institute or order a proceeding . . ., the Director ***may*** take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office.” We are not required by statute to reject a petition based upon the fact that certain arguments or art were considered previously by the Office, and we decline to do so in this case.

Next, Patent Owner argues that the “combination of Nolan with the SCSI-2 Specification fails to disclose any ‘distinguishing’ of signals *within a data stream*, because, by design, the SCSI target controls the transmission of data versus command signals separately on the DATA BUS, so no ‘distinguishing’ is required.” Prelim. Resp. 27 (emphasis added). Patent

Owner adds that only one kind of signal is present on the data bus during a particular phase. *Id.* at 28–29.

We understand Patent Owner's argument to be that both control/command signals and data signals must be present within the same data stream in order to satisfy the limitation of "at least one data stream interceptor that distinguishes between command/control and data signal transfers" recited in claim 9. Prelim. Resp. 27–29. Although we have construed the data stream interceptor to "distinguish the command or control signals *in the data stream* from the data signals," our construction does not require that both the command/control signals and data signals must be present in the same data stream for the data stream interceptor to perform the recited function. Thus, based on the current record, we are persuaded by Petitioner's argument that Nolan's SCSI Interface 15 combined with SCSI-2's C/D signal meets this limitation.

Claim 9 further recites "a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor." Ex. 1001, 6:48–52. Petitioner argues Nolan's disclosure of microprocessor 17 receiving input from SCSI Interface 15 meets this limitation. Pet. 23–24. Petitioner explains that Nolan's Figure 1 shows that microprocessor 17 receives input from SCSI Interface 15. *Id*. at 24. Petitioner's declarant, Dr. Long, adds "SCSI bus 13 connects host computer 12 to SCSI Interface 15 and transfers data through SCSI bus 13 using the SCSI protocol." Ex. 1006 ¶ 124 (citing Ex. 1002, Fig. 1, 4:17–26). Petitioner further argues Figure 2 of Nolan shows a flowchart with a "WAIT FOR INPUT SCSI COMMAND." Pet.

24. Petitioner explains that microprocessor 17 receives the input SCSI command from SCSI Interface 15, and "whenever input received from SCSI Interface 15 indicates a data transfer (step 36), microprocessor 17 makes a determination as to whether encryption or decryption is required (step 37)." *Id.* at 24–25.

Patent Owner argues Nolan does not disclose how the input SCSI command is received by microprocessor 17 because Figure 1 does not show SCSI Commands are sent from host computer 12 to microprocessor 17 by SCSI Interface 15. Prelim. Resp. 33–34. Patent Owner additionally argues that, even if host SCSI commands were received by microprocessor 17, "Petitioner provides no link disclosed in Nolan between the allegedly received input and the determination to encrypt, decrypt, or pass through." *Id.* at 35. Patent Owner also contends Petitioner's declarant, Dr. Long, is mistaken in implying that the claimed determination can be performed based "solely on whether or not the information is data or command/status." *Id.* at 37. Patent Owner asserts that "the mere fact that data is being transferred does not mean" the data should be encrypted/decrypted. *Id.* at 36.

Based on the current record, we are persuaded Petitioner has explained sufficiently how Nolan discloses data transfer between host computer 12 to microprocessor 17 through SCSI Interface 15 and SCSI bus 13. Pet. 24. Moreover, we are persuaded by Petitioner that Nolan's Figure 2 shows a microprocessor making a determination for encryption or decryption based on the input SCSI command. *Id.* at 25. For example, Nolan discloses that, if the "command" involves tape movement, the "microprocessor then ascertains whether any transfer of encrypted data is required, steps 36 and 37." Ex. 1002, 6:24–25.

Further, we are not persuaded by Patent Owner's argument that the claimed determination cannot be based solely on whether the information is data or command/status. The broadest reasonable construction of the term "input" does not require a specific kind of input that excludes whether information is data, command, or status. *See supra* Claim Construction. Thus, based on the current record, we conclude Petitioner has explained sufficiently how the alleged teachings in Nolan and SCSI-2 meet the recited main controller limitation.

Claim 9 also recites "at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller." Ex. 1001, 6:53–56. Petitioner argues that SCSI Interface 15 meets this limitation, because Nolan states that host computer interface 15 (also called SCSI Interface 15) "can, under the control of the microprocessor 17, transfer data directly to or from a host memory buffer 18." Pet. 26 (citing Ex. 1002, 4:27–5:1). Petitioner adds that SCSI Interface 15 performs a data transfer protocol with the data generating device (host computer 12) on command from the main controller (microprocessor 17). *Id.* (citing Ex. 1006 ¶ 24). Based on the current record, we are persuaded by Petitioner's arguments.

Claim 9 further recites "at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller." Ex. 1006, 6:56–60. Petitioner asserts SCSI Interface 16 transfers data between the tape storage medium and host memory buffer or target memory buffer under the control of microprocessor 17. Pet. 27 (citing Ex. 1002, 5:1–4). Petitioner explains that "SCSI Interface 16 in Nolan (also called target tape drive interface 16),

when implemented using the SCSI-2 Specification, performs a data transfer protocol with the data storage device (tape storage medium 11) on command from the main controller (microprocessor 17)." *Id.* (Ex. 1006 ¶ 128). Based on the current record, we are persuaded Petitioner has shown sufficiently that the teachings in Nolan satisfy this limitation.

Claim 9 also recites "at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller." Ex. 1001, 6:61–64. Petitioner argues "Nolan discloses a cipher engine—encryption block 20—situated within Nolan's cryptographic device ("apparatus 10") between the data generating device (host computer 12) and the data storage device (tape storage medium 11)." Pet. 29. Petitioner's declarant, Dr. Long, testifies that encryption block 20 performs data transfers transparently, because "[l]ike the cipher engine in the '995 Patent, Nolan's encryption block 20 has its own dedicated microprocessor 17 as part of the encryption/decryption apparatus 10," and "Nolan's cryptographic device uses the SCSI bus lines 13 and 14 that normally would have connected the host computer 10 directly to tape storage drive 11 without alteration." *Id*. at 30 (quoting Ex. 1006, ¶ 133). Applying our claim construction for the term "transparently," we are persuaded by Petitioner's assertion that the disclosure in Nolan meets the cipher engine limitation.

Patent Owner contends that secondary considerations of obviousness, such as evidence of commercial success, praise by others, and copying by others, "heavily weighs against" finding the '995 patent obvious. Prelim. Resp. 43–45. The issue of secondary considerations is highly fact-specific,

and at this stage of the proceeding, the record regarding such secondary considerations is incomplete. For example, Patent Owner does not establish that its products, e.g., the MX and X-Wall products (Pet. 43–44), are directed to the claimed subject matter recited in claim 1–15. Nor does Patent Owner direct us to expert testimony that establishes a connection between its products that allegedly embody the claimed invention and claimed subject matter recited in claims 1–15. In the absence of an established nexus with the claimed invention, Patent Owner's allegation of commercial success, praise by others, and copying are entitled to little weight, and generally have no bearing on the legal issue of obviousness. *See In re Vamco Machine & Tool, Inc.*, 752 F.2d 1564, 1577 (Fed. Cir. 1985). Therefore, we determine that Patent Owner's evidence of commercial success is insufficient to preclude instituting this proceeding. Our determination in that regard does not prevent Patent Owner from further developing such evidence during this proceeding.

In sum, upon review of Petitioner's analysis and supporting evidence, as well as the arguments presented in the Preliminary Response, we conclude Petitioner has demonstrated a reasonable likelihood it will prevail with respect to claim 9. In addition, Petitioner provides detailed explanations of how each limitation of claims 1–8 and 10–13 is taught or suggested by the combination of Nolan and SCSI-2. Pet. 52–58. Those contentions have merit. Thus, based on the current record, Petitioner has demonstrated a reasonable likelihood it will prevail with respect claims 1–8 and 10–13 on this ground.

C. Claim 14 – Obviousness over Nolan, SCSI-2, and Hamlin (Ex. 1004)

Petitioner argues claim 14 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Hamlin. Pet. 40–44. Specifically, Petitioner contends claims 13 and 14 contain the same limitations, except that claim 14's preamble recites "[a] cryptographic device *integrated within a data storage device for use during data transfer with a data generating device*." *Id*. at 40 (emphasis added). As discussed above, we treat the preamble as limiting claim 14. *See supra* Claim Construction.

1. Summary of Hamlin (Ex. 1004)

Hamlin is directed to the "need for a disk drive comprising a tamper resistant cryptosystem which is protected from an attacker employing chosen plaintext attacks." Ex. 1004, 2:3–5. Hamlin discloses "a disk drive comprising a disk for storing encrypted data." Ex. 1004, Abstract. Hamlin teaches second circuit 100, including encryption circuitry 110, that is housed within the disk drive. *Id.* at 2:66–3:3, Fig. 1.

2. Analysis

Petitioner argues Hamlin discloses encryption circuitry 110 connected to interface 104, which is "connected to receive user data from a host computer." Pet. 44 (citing Ex. 1004, Fig. 2, 4:18–22). Petitioner further asserts encryption circuit 110 is housed within disk drive, which is a data storage device. *Id*. at 43. Petitioner asserts that a person of ordinary skill in the art would have recognized the physical security of Nolan's cryptographic device (implemented using the SCSI-2 Specification), and particularly access to Nolan's SCSI bus, could be enhanced by housing Nolan's cryptographic device within a storage device, as taught by Hamlin. *Id.* at 44.

Patent Owner reiterates that Nolan and SCSI-2 do not disclose the

recited data stream interceptor or main controller, and Hamlin does not supply the missing teaching. Prelim. Resp. 41. For the same reasons discussed above, we are persuaded by Petitioner's contentions that the teachings in Nolan and SCSI-2 satisfy the data stream interceptor and main controller limitations recited in claim 14. We also are persuaded Petitioner has explained sufficiently how the combination of Nolan, SCSI-2, and Hamlin teach or suggest the remaining limitations of claim 14. Based on the current record, we are persuaded Petitioner has established a reasonable likelihood of prevailing on this ground.

D. Claim 15 – Obviousness over Nolan, SCSI-2, and Detrick (Ex. 1005)

Petitioner argues claim 15 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Detrick. Pet. 44–49. Specifically, Petitioner contends claims 13 and 15 contain the same limitations except that claim 15's preamble recites "a cryptographic device *integrated within a data generating device for use during data transfer with a data storage device*." *Id*. at 45 (emphasis added). As discussed above, we treat the preamble as limiting claim 15. *See supra* Claim Construction.

1. Summary of Detrick (Ex. 1005)

Detrick is directed to "implementing encryption and decryption of data stored from a computer system to a storage medium." Ex. 1005, 1:9–10. Figure 1 (reproduced below) shows an "embodiment of a computing system implementing encryption/decryption capabilities." *Id.* at 2:61–63.

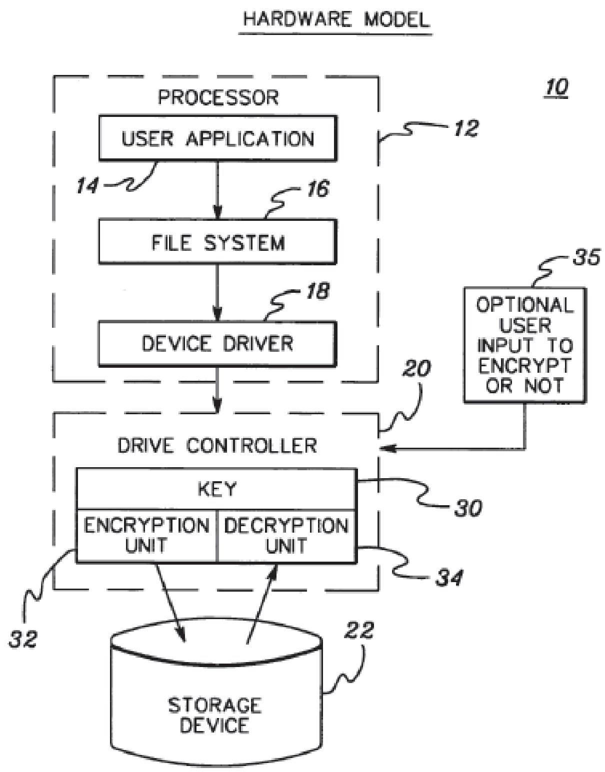


fig. 1

Figure 1 shows computing system 10 with processor 12 and drive controller 20. "The hardware encryption and decryption could be either in the drive controller 20 (as shown), or in the drive itself." *Id.* at 3:50–52. Detrick states driver controller 20 can "regulate the flow of data to and from a disk drive, floppy drive, etc." *Id.* at 3:65–67. Detrick discloses "[c]ommon types of drive controllers include . . . SCSI." *Id.* at 4:1–2.

2. Analysis

Petitioner asserts Figure 1 of Detrick shows encryption/decryption hardware housed within a data generating device. Pet. 48. Petitioner's declarant, Dr. Long, testifies:

> [a] person of ordinary skill in the art at the time of the filing of the '995 Application would have recognized from the teachings of Detrick that the physical security of Nolan's cryptographic

> device (implemented using the SCSI-2 Specification), and particularly access to Nolan's SCSI bus, could be enhanced by housing Nolan's cryptographic device within a data generating device such as a computer.

Id. at 48–49 (quoting Ex. 1006 ¶ 193).

Patent Owner argues again that Nolan and SCSI-2 does not disclose the recited data stream interceptor or main controller, and Hamlin does not supply the missing teaching. Prelim. Resp. 42. For the same reasons discussed above, we are persuaded by Petitioner's contentions that the teachings in Nolan and SCSI-2 satisfy the data stream interceptor and main controller limitations recited in claim 15. We also are persuaded Petitioner has explained sufficiently how the combination of Nolan, SCSI-2, and Detrick teach or suggest the remaining limitations of claim 15. Based on the current record, we are persuaded Petitioner has established a reasonable likelihood of prevailing on this ground.

E. Other Grounds of Unpatentability Asserted under 35 U.S.C. § 103(a)

Petitioner additionally challenges claims 14 and 15 on the ground that the claims are unpatentable under 35 U.S.C. § 103(a) over Nolan and SCSI-2. Pet. 40–42, 45–47. We determine this ground is redundant to the grounds of unpatentability on which we institute *inter partes* review for the same claims. Accordingly, we exercise our discretion not to authorize an *inter partes* review on the remaining ground of unpatentability asserted by Petitioner against claims 14 and 15 of the '995 patent. *See* 37 C.F.R. § 42.108(a).

III. CONCLUSION

For the foregoing reasons, we are persuaded the information presented in the Petition establishes there is a reasonable likelihood Petitioner would prevail with respect to claims 1–15.

We have not made a final determination on the patentability of any challenged claims.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the ’995 patent is hereby instituted as to claims 1–15 of ’995 patent for the following grounds:

A. Claims 1–13 are unpatentable under 35 U.S.C. § 103(a) over Nolan and SCSI-2;

B. Claim 14 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Hamlin; and

C. Claim 15 is unpatentable under 35 U.S.C. § 103(a) over Nolan, SCSI-2, and Detrick;

FURTHER ORDERED that the trial is limited to the grounds identified above and no other grounds are authorized; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial is commencing on the entry date of this decision.

PETITIONER:

Richard Marsh
Richard.marsh@faegreBD.com

Christopher Larson
Chris.larson@faegreBD.com

PATENT OWNER:

Hector J. Ribera
hribera@fenwick.com

Natu J. Patel
npatel@thepatellawfirm.com

EXHIBIT 1001

US007136995B1

(12) **United States Patent**
Wann

(10) **Patent No.: US 7,136,995 B1**
(45) **Date of Patent: Nov. 14, 2006**

(54) **CRYPTOGRAPHIC DEVICE**

(75) Inventor: **Shuning Wann**, Taipei (TW)

(73) Assignee: **Enova Technology Corporation**, Taipei (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1017 days.

(21) Appl. No.: **09/704,769**

(22) Filed: **Nov. 3, 2000**

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/153**; 713/190; 713/192; 380/42; 902/2; 705/64; 705/73

(58) **Field of Classification Search** 380/42; 713/153, 192, 190, 260, 200; 902/2; 705/64, 705/73
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,780,905 A * 10/1988 Cruts et al. 380/44
5,513,262 A * 4/1996 van Rumpt et al. 380/29
6,081,895 A * 6/2000 Harrison et al. 713/189

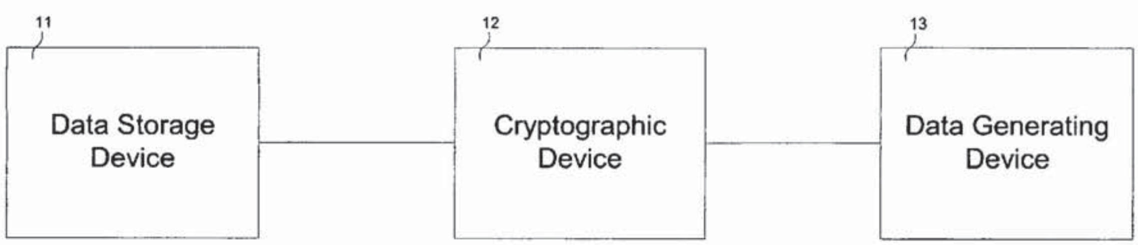
* cited by examiner

Primary Examiner—Emmanuel L. Moise
Assistant Examiner—Paul Callahan
(74) *Attorney, Agent, or Firm*—The Patel Law Firm, P.C.; Natu J. Patel

(57) **ABSTRACT**

A cryptographic device comprises a data stream interceptor, a main controller receiving input from the data stream interceptor, and a pair of data generating and storage controllers adapted to perform data transfer protocols with corresponding peer controllers of a data generating device and a data storage device, respectively, on command from the main controller. The cryptographic device further comprises a cipher engine programmed to transparently encrypt and decrypt data streams flowing between the data generating device and data storage device on command from the main controller. The cryptographic device does not utilize system resources associated with the data generating and storage devices during operation.

15 Claims, 4 Drawing Sheets



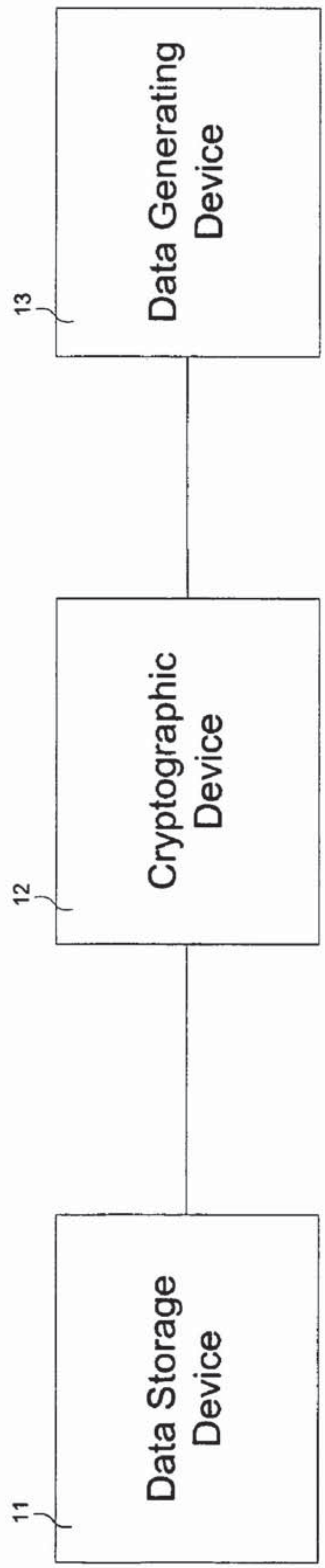

Data Generating Device
13
Cryptographic Device
12
Data Storage Device
11

FIG. 1

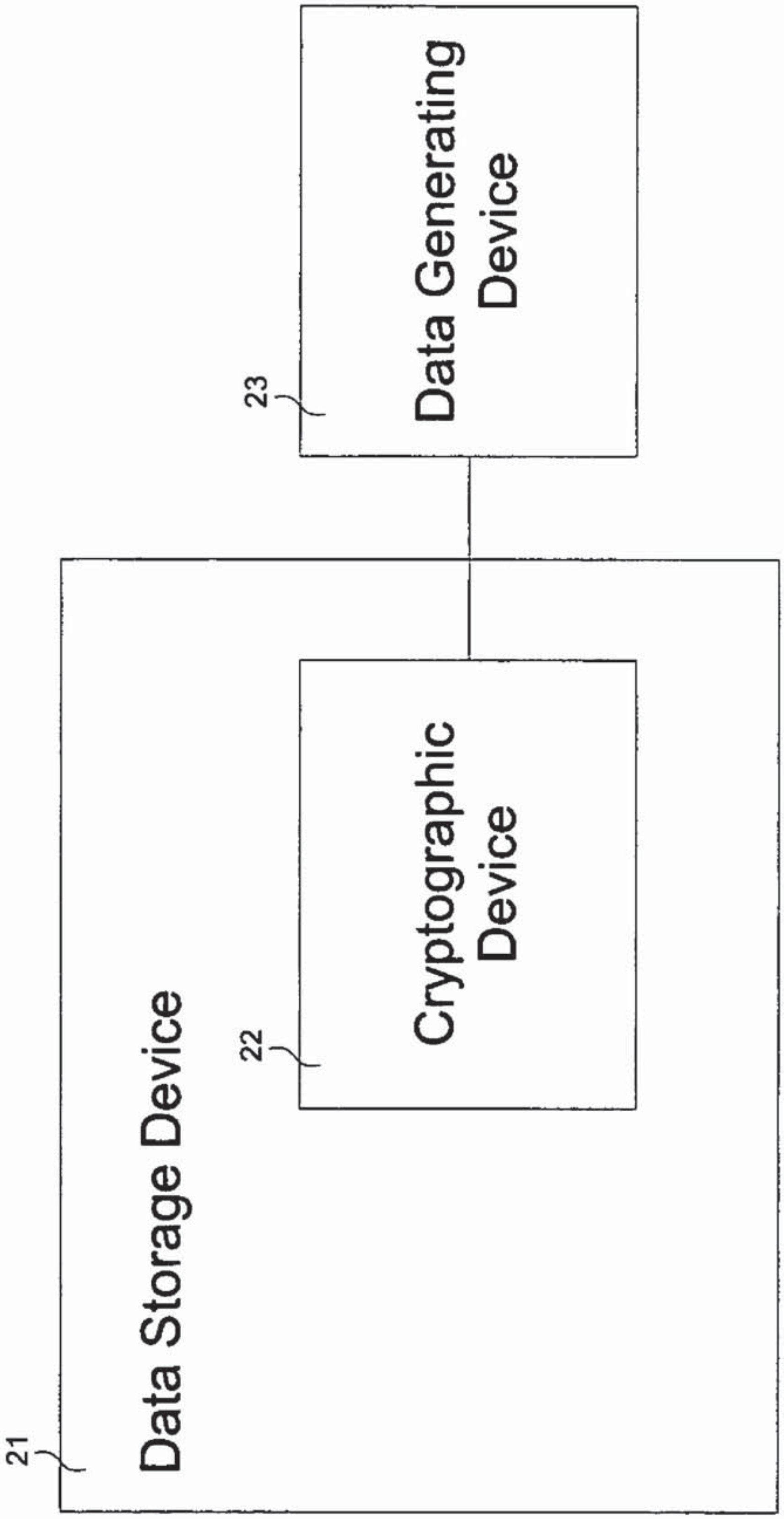

Data Generating Device
23
Cryptographic Device
22
Data Storage Device
21

FIG. 2

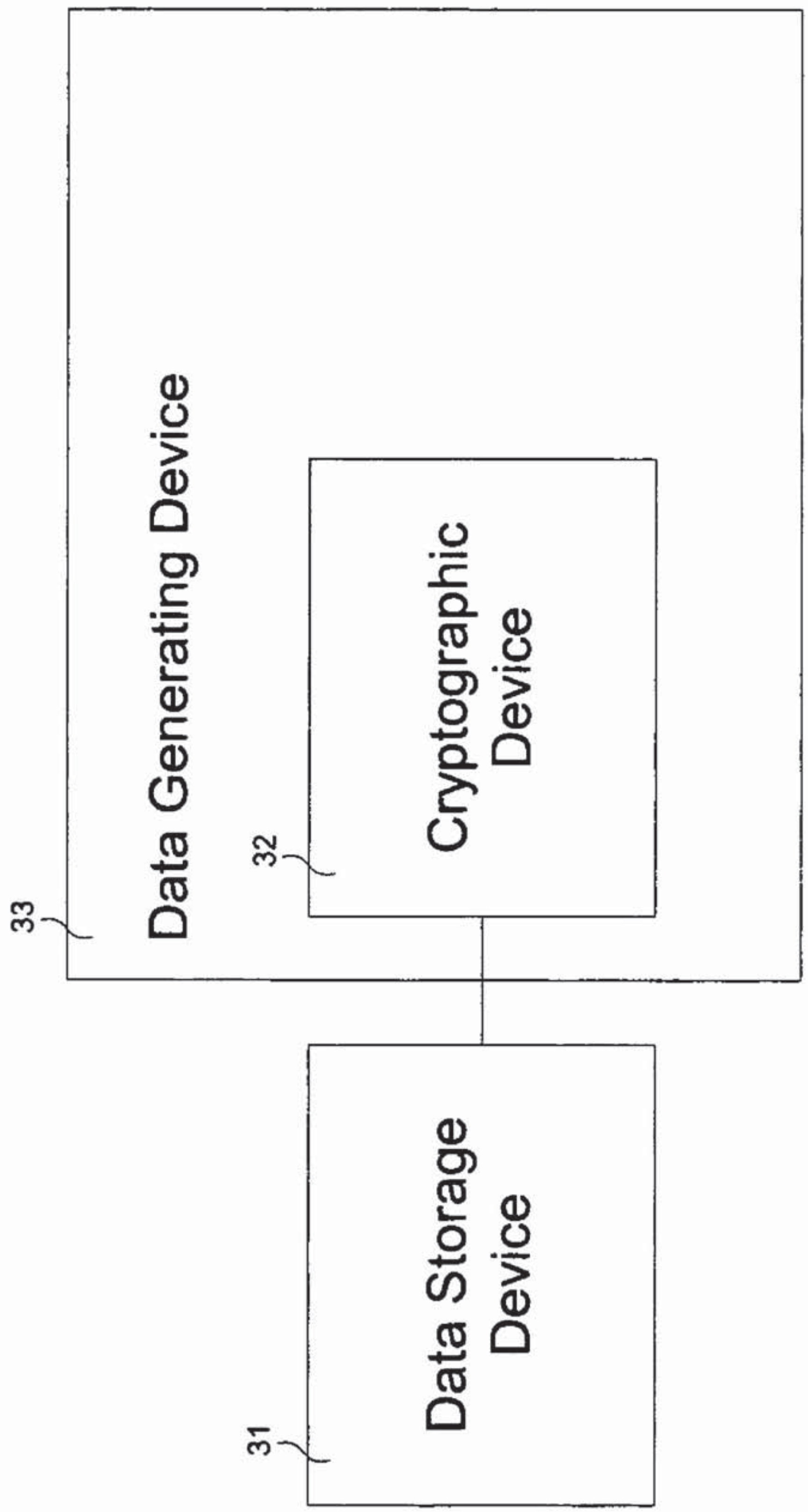

Data Generating Device
33
Cryptographic Device
32
Data Storage Device
31

FIG. 3

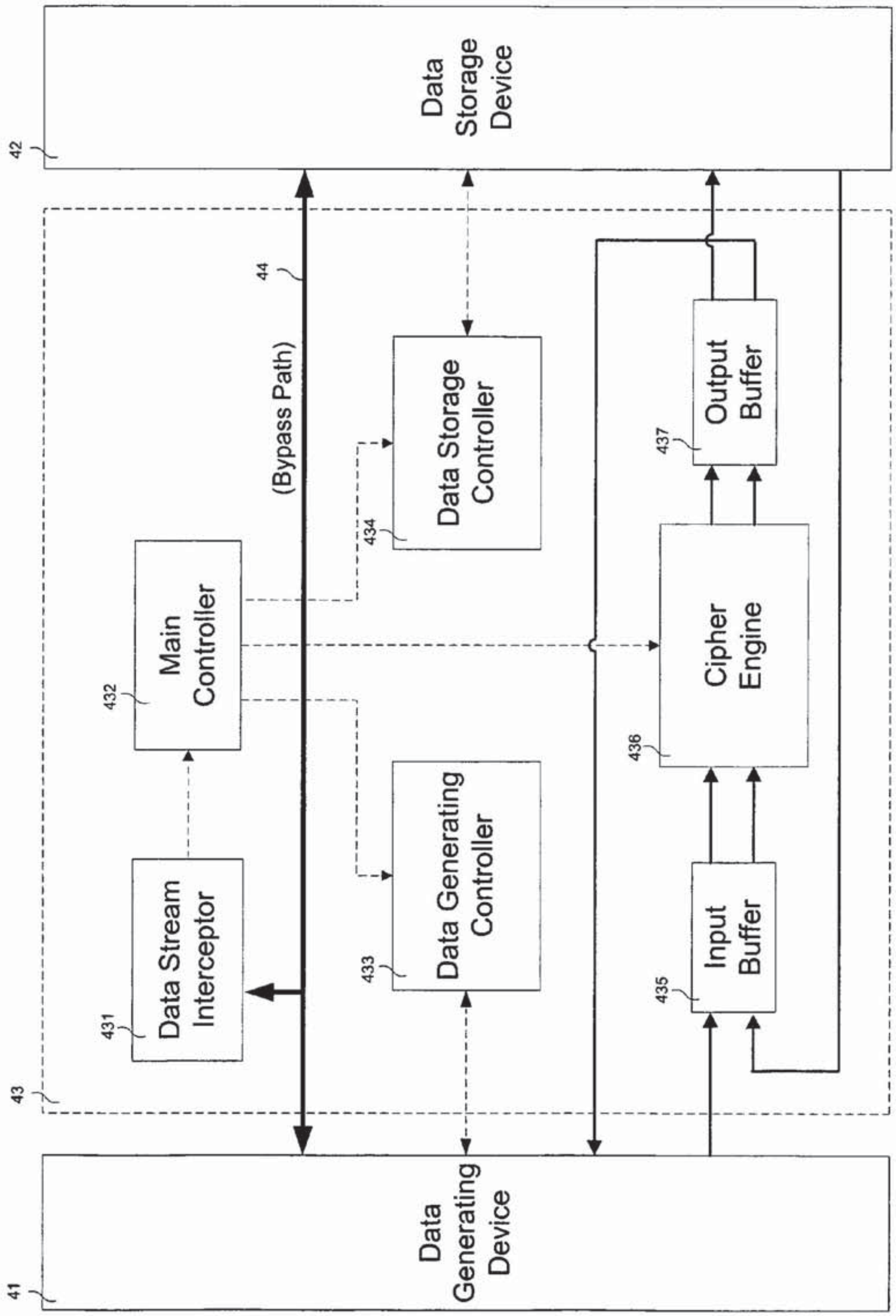

42
Data Storage Device
43
44
(Bypass Path)
431
Data Stream Interceptor
432
Main Controller
433
Data Generating Controller
434
Data Storage Controller
435
Input Buffer
436
Cipher Engine
437
Output Buffer
41
Data Generating Device

FIG. 4

CRYPTOGRAPHIC DEVICE

FIELD OF THE INVENTION

The present invention relates generally to cryptography and more particularly to a device adapted to perform data encryption/decryption without compromising the overall system performance.

BACKGROUND OF THE INVENTION

Encryption is a security technology designed to preserve the privacy and confidentiality of sensitive data that is being stored or transmitted. Sensitive data is routinely stored unencrypted on desktop computers, workstations, notebooks, personal digital assistants (PDAs), cellular telephones, and the like. The hard drives of notebooks are especially at risk as the computers are frequently used in non-secure environments and may be relatively easily removed by an unauthorized user. Computer hard drives may contain strategic data, patent applications, patent drawings, litigation documents, consumer lists, private health care information, payroll data and other types of sensitive data. Users frequently store unencrypted passwords and access codes to corporate networks on notebooks, which may compromise corporate network security. Statistics compiled annually by the FBI show that network security breaches are to a significant extent being perpetrated by employees or contractors who have or can gain access to sensitive data on an intranet. Moreover, unattended desktop PCs become frequent targets for unauthorized users attempting to gain illicit entry into a private network.

Comparatively few cryptographic applications have been developed to protect data, with most of the applications being software-based applications adapted to perform file-level cryptography. File-level cryptography can also be done by various hardware devices such as PCMCIA cards or external ASIC-based devices. On the surface, encrypting only selected files instead of entire hard drives seems to make sense since not all data is confidential. However, file cryptography is inherently slow because the entire file must be decrypted before any portion of the file can be presented to the user. Also, file encryption normally ignores the temporary and swap files that are automatically created and stored in clear text on the hard drive. Worse still, file encryption frequently results in compromised overall system performance, and requires manual intervention by users who may become confused and frustrated by the number of requisite interactive steps embedded in the application. From an organizational point of view, the lack of automatic and transparent cryptographic operation makes it inherently difficult to enforce data security policies on computers, mobile communication devices and networks alike. Furthermore, the level of security attainable with file-level cryptography is questionable, since file encryption programs run under the control of the computer operating system (OS) and the OS lacks sufficient access control. If an unauthorized user were capable of subverting the OS, subverting the file-level cryptography application would be entirely feasible as well. Although PCMCIA encryption cards and external ASIC encryption devices have been designed to provide greater key security and to improve performance, these devices have had only marginal success and suffer from a variety of compatibility issues. It, therefore, becomes increasingly clear that conventional cryptography applica-

tions are not suitable for organizations and/or individuals requiring optimized security, convenience and uncompromised system performance.

SUMMARY OF THE INVENTION

The present invention is generally directed to a cryptographic device adapted to perform data encryption and decryption on at least one data stream flowing between at least one data generating device and at least one data storage device without compromising overall system performance.

In one embodiment of the present invention, the cryptographic device is adapted to intercept at least one data stream flowing between the data generating device and the data storage device, and transparently perform data encryption and decryption in accordance with the intercepted data stream.

In another embodiment of the present invention, the cryptographic device comprises a data stream interceptor, a main controller receiving input from the data stream interceptor, a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from the main controller, a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from the main controller, and a cipher engine adapted to transparently encrypt and decrypt data streams flowing between the data generating device and the data storage device on command from the main controller.

Another preferred embodiment is to place, between the Main Control and the Signal Transmission Line, an Interceptive Device for intercepting data to be encrypted or decrypted according to the Main Control instructions.

Yet another preferred embodiment is to introduce two Data Buffers, one of which is provided between the data encryption-decryption device and the data storage device, and the other buffer provided between the data encryption-decryption device and the data-generating device, for storing pre-decrypted and encrypted data and pre-encrypted and decrypted data, respectively.

These and other aspects of the present invention will become apparent from a review of the accompanying drawings and the following detailed description of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is best understood from the following detailed description when read in conjunction with the accompanying drawings. It is emphasized that, according to common practice, the various features of the drawings are not to scale with dimensions of the various features being arbitrarily expanded or reduced for clarity. Like numerals denote like features throughout the specification and drawings in which:

FIG. **1** schematically depicts a cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer;

FIG. **2** schematically depicts a data storage device with an integral cryptographic device operatively coupled to a data generating device for use during data transfer;

FIG. **3** schematically depicts a data generating device with an integral cryptographic device operatively coupled to a data storage device for use during data transfer; and

FIG. **4** schematically depicts the architecture of a cryptographic device in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Some embodiments of the present invention are described in detail with reference to the related drawings of FIGS. **1**–**4**. Additional embodiments, features and/or advantages of the invention will become apparent from the ensuing description or may be learned by practicing the invention.

FIG. **1** schematically depicts a cryptographic device **12** operatively coupled between a data generating device **13** and a data storage device **11** for use during data transfer. In general, data generating device **13** may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data, while data storage device **11** may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device **12** is adapted to perform data encryption/decryption during data transfers between data generating device **13** and data storage device **11** without compromising the overall system performance. Specifically, cryptographic device **12** does not utilize resources typically associated with data generating device **13**, such as CPU, DRAM, or other system resources during data transfers between data generating device **13** and data storage device **11**. From the functional viewpoint of data generating device **13** and/or data storage device **11**, data transfers are being performed directly between data generating device **13** and/or data storage device **11**, respectively, without any intervention by cryptographic device **12**. In general, cryptographic device **12** acts as an "invisible" data transfer bridge connecting data generating device **13** and data storage device **11**. Cryptographic device **12** may be implemented in any suitable stand-alone hardware form such as a hub or the like. Cryptographic device **12** may also be implemented as a designated data transfer interface adapted to use various data communication protocols in network applications such as local area networks (LANs), wide area networks (WANs), and the like.

FIG. **2** schematically depicts a data storage device **21** with an integral cryptographic device **22** being operatively coupled to a data generating device **23** for use during data transfer. Cryptographic device **22** may be integrated in ASIC chip form on the front end of the data transfer interface (not shown) of data storage device **21** without any modification of dataflow control hardware, drivers or data storage device **21** itself. The data transfer interface may be in the form of Socket, IDE, PCI, **1394**, SCSI, PCMCIA, USB or any other suitable data transfer interface. In general, data generating device **23** may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device **21** may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device **22** is programmed to perform transparently data encryption/decryption during data transfers between data generating device **23** and data storage device **21** without compromising the overall system performance. From the functional viewpoint of data generating device **23**, data transfer is being performed directly with data storage device **21** without any apparent intervention by integral cryptographic device **22**.

FIG. **3** schematically depicts a data generating device **33** with an integral cryptographic device **32** being operatively coupled to a data storage device **31** for use during data transfer. Cryptographic device **32** may be integrated in ASIC chip form on the front end of the data transfer interface (not shown) of data generating device **33** without any modification to dataflow control hardware, drivers or data generating device **33** itself. The data transfer interface may be in the form of Socket, IDE, PCI, 1394, SCSI, PCMCIA, USB or any other suitable data transfer interface. In general, data generating device **33** may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device **31** may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device **32** is programmed to perform transparently data encryption/decryption during data transfers between data generating device **33** and data storage device **31** without compromising the overall system performance. From the functional viewpoint of data storage device **31**, data transfer is being performed directly with data generating device **33** without any apparent intervention by integral cryptographic device **32**.

FIG. **4** depicts schematically the architecture of a cryptographic device **43** in accordance with the present invention. In the embodiment of FIG. **4**, cryptographic device **43** is shown operatively coupled between a data generating device **41** and a data storage device **42** for use during data transfer. In general, data generating device **41** may be a desktop/notebook computer, microprocessor, hub, router, mobile computing device, interface card, or any other device capable of generating data. Data storage device **42** may be a computer hard drive, tape drive, floppy diskette, compact disk drive, magnetic optical drive, digital video recorder, flash memory card, magnetic tape, compact disk (CD), CD-RW, CD+RW, CD-R, digital versatile disk, PCMCIA card, or any other device capable of storing data for retrieval purposes. Cryptographic device **43** may be implemented in any suitable hardware form. Cryptographic device **43** is adapted to perform transparently data encryption and decryption during data transfers between data generating device **41** and data storage device **42** with no impact on overall system performance.

As generally illustrated in FIG. **4**, cryptographic device **43** comprises a data stream interceptor **431** which is operatively coupled to a main controller **432**. Main controller **432** communicates control signals to a data generating controller **433**, a data storage controller **434**, and a cipher engine **436**. Main controller **432** receives input from data stream interceptor **431** and determines whether an incoming data stream, which may include command/control and/or data signals, is to be encrypted, decrypted or passed through unmodified. In this regard, data stream interceptor **431** is adapted to distinguish between command/control and data signal transfers. Specifically, interceptor **431** is configured to pass through certain command/control signals via a bypass data path **44**, and intercept other command/control signals which are transmitted to main controller **432**, as generally depicted in FIG. **4**. Main controller **432** instructs data generating controller **433** and data storage controller **434** to perform specific data transfer protocols such as read/write, PIO/

DMA, ATA/IDE, PCI, and the like with corresponding peer controllers (not shown) of data generating device **41** and data storage device **42**, respectively, according to the intercepted command/control signals. Main controller **432** also transmits control signals to cipher engine **436** to notify the same of an incoming data stream. Cipher engine **436** is operatively coupled between an input buffer **435** and an output buffer **437**, and programmed to transparently encrypt/decrypt streaming data during data transfer between data generating device **41** and data storage device **42**, as generally shown in FIG. **4**. Input buffer **435** stores pre-encrypted and pre-decrypted data, while output buffer **437** stores encrypted and decrypted data, respectively. Input buffer **435** receives data from data generating device **41** or data storage device **42** depending on the type of data transfer. Output buffer **437** outputs data to data generating device **41** or data storage device **42** depending on the type of data transfer. Data generating device **41** may include a 1-bit, 8-bit, 16-bit or 32-bit data width interface. Data storage device **42** may include a 1-bit, 8-bit, 16-bit or 32-bit data width interface. Cipher engine **436** may include a 64-bit, 128-bit or other data width interface depending on the ciphering algorithm being used. Input buffer **435** is adapted to convert incoming data width to a data width suitable for input to cipher engine **436**. Output buffer **437** is adapted to convert incoming data width to a data width suitable for output to data storage device **42** or data generating device **41**.

No resources associated with data generating device **41** or data storage device **42**, or any other system resources, are being used by cryptographic device **43** during data transfer between data generating device **41** and data storage device **42**. Cryptographic device **43** independently and transparently encrypts/decrypts incoming data streams without compromising the overall system performance. A person skilled in the art would recognize that cryptographic device **43** may be adapted for implementation in network communication applications such as those involving LANs, WANs, virtual private networks (VPNs), and the Internet.

While the invention has been described in terms of various specific embodiments, those skilled in the art would recognize that the invention can be practiced with modification within the spirit and scope of the claims. Additionally, features illustrated or described as part of one embodiment can be used in another embodiment to provide yet another embodiment such that the features are not limited to the specific embodiments described hereinabove. Thus, it is intended that the present invention cover all such embodiments and variations as long as such embodiments and variations come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A cryptographic device, compromising:

at least one data stream interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted or passed through based on the received input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

2. The cryptographic device of claim **1**, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

3. The cryptographic device of claim **2**, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

4. The cryptographic device of claim **2**, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

5. A cryptographic device, comprising:

at least one data stream interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be decrypted or passed through based on the received input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

6. The cryptographic device of claim **5**, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

7. The cryptographic device of claim **6**, wherein said at least one input buffer receives data input from said at least one data generating device and said at least one data storage device.

8. The cryptographic device of claim **6**, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

9. A cryptographic device, comprising:

at least one data stream interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt or decrypt at least one data stream between said at least one data generating device and said at least one data storage device on command from said main controller.

10. The cryptographic device of claim **9**, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

11. The cryptographic device of claim 10, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

12. The cryptographic device of claim 10, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

13. A cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer, said cryptographic device comprising:

a data steam interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said at least one data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt or decrypt at least one data stream between the data generating device and the data storage device on command from said main controller.

14. A cryptographic device integrated within a data storage device for use during data transfer with a data generating device, said cryptographic device comprising:

a data stream interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt or decrypt at least one data stream between the data generating device and the data storage device on command from said main controller.

15. A cryptographic device integrated within a data generating device for use during data transfer with a data storage device, said cryptographic device comprising:

a data stream interceptor that distinguishes between command/control and data signal transfers;

a main controller receiving input from said data stream interceptor and determining whether incoming data would be encrypted, decrypted or passed through based on the received input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt or decrypt at least one data stream between the data generating device and the data storage device on command from said main controller.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,136,995 B1
APPLICATION NO. : 09/704769
DATED : November 14, 2006
INVENTOR(S) : Shuning Wann

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 5, line 52, claim 1 "compromising" should read --comprising--.

Column 6, line 57, claim 9 "on" should read --one--.

Signed and Sealed this

Twenty-third Day of February, 2010

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

CERTIFICATE OF SERVICE

I, Nickou Oskoui, certify that on this, the 18th day of April, 2016, I caused the foregoing Opening Brief of Appellant Enova Technology Corporation to be filed with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF system, which will send notice of such filing to all registered CM/ECF users, including opposing counsel of record in this appeal:

Calvin L. Litsey David J.F. Gross Lucas J. Tomsich Faegre Baker Daniels 1950 University Ave., Suite 450 East Palo Alto, CA 94303	**[X] By Email**: calvin.litsey@faegrebd.com david.gross@faegrebd.com lucas.tomsich@faegrebd.com
Richard M. Marsh, Jr. (Reg. No. 59,031) Faegre Baker Daniels LLP 3200 Wells Fargo Center 1700 Lincoln Street Denver, CO 80203	**[X] By Email:** richard.marsh@faegrebd.com
Julie B. Wahlstrand Faegre Baker Daniels LLP 2200 Wells Fargo Center 90 S. Seventh Street Minneapolis, MN 55402-3901	**[X] By Email**: julie.wahlstrand@faegrebd.com

Dated: April 18, 2016

Respectfully submitted,

/s/ *Nickou Oskoui*

Nickou Oskoui
VINSON & ELKINS LLP
2001 Ross Avenue, Suite 3700
Dallas, TX 75201-2975
Telephone: (214) 220-7700
Facsimile: (214) 220-7716
Email: noskoui@velaw.com

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B).

 X The brief contains 13,975 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii), or

____ The brief uses a monospaced typeface and contains ________ lines of text, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6).

 X The brief has been prepared in a proportionally spaced typeface using MS Word 2010 in a 14-point Times New Roman font or

____ The brief has been prepared in a monospaced typeface using ________ _________________in a ___ characters per inch_________ font.

Dated: April 18, 2016

Respectfully submitted,

/s/ *Darryl M. Woo*
DARRYL M. WOO
VINSON & ELKINS LLP

Counsel for Appellant Enova Technology Corporation